(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2001136161 A

(43) Date of publication of application: 18.05.01

(51) Int. Cl H04L 9/08
G06F 12/14
G09C 5/00

(21) Application number: 2000248195

(22) Date of filing: 18.08.00

(30) Priority: 20.08.99 JP 11233813
20.08.99 JP 11233815
20.08.99 JP 11233814

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

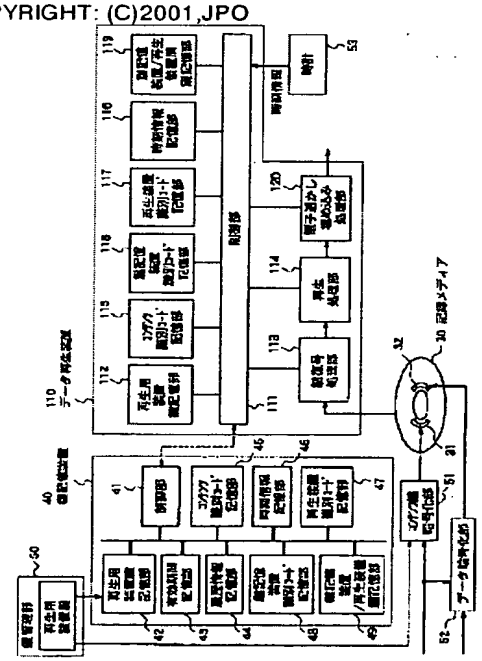
(72) Inventor: KAWADA KOJI
KATSUTA NOBORU
IBARAKI SUSUMU
TATEBAYASHI MAKOTO
HARADA TOSHIHARU

(54) DATA REPRODUCTION DEVICE, DIGITAL CONTENTS REPRODUCTION DEVICE, REPRODUCTION SYSTEM, INFORMATION IMBEDDING DEVICE AND IMBEDDED INFORMATION DETECTOR

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a data reproduction device and a reproduction system that can prevent illegal reproduction of data due to an illegal access by a person not qualified for reproduction and an illegal operation of time information and to provide an information imbedding device and an imbedded information detector that can realize detection and prevention of an illegal use of a literary work such as illegal copy.

SOLUTION: A control section 111 of a data reproduction device 110 outputs a key request command including time information or the like to a key storage device 40 having a reproduction device key generated by each data reproduction device 110, the key storage device 40 receiving the command confirms whether or not the access is illegal on the basis of the information included in the command, records a key read history, delivers the key to the data reproduction device 110, which imbeds the key read history in a form of an electronic watermark to data decoded by using the key and outputs the resulting data.



(19) 日本国特許庁 (JP)

(12) 公開特許公報（A）

(11) 特許出願公開番号

特開２００１－１３６１６１
(P2001-136161A)
(43) 公開日 平成13年5月18日(2001.5.18)

(51)Int.Cl.[7]	識別記号	FI		テーマコード(参考)
H04L 9/08		G06F	12/14	310 Z
G06F 12/14	310			320 C
	320			320 F
		G09C	5/00	
G09C 5/00		H04L	9/00	601 C

審査請求 未請求 請求項の数 29 OL （全 27 頁） 最終頁に続く

(21) 出願番号 特願2000-248195(P2000-248195)

(22) 出願日 平成12年8月18日(2000.8.18)

(31) 優先権主張番号 特願平11-233813
(32) 優先日 平成11年8月20日(1999.8.20)
(33) 優先権主張国 日本（ＪＰ）
(31) 優先権主張番号 特願平11-233815
(32) 優先日 平成11年8月20日(1999.8.20)
(33) 優先権主張国 日本（ＪＰ）
(31) 優先権主張番号 特願平11-233814
(32) 優先日 平成11年8月20日(1999.8.20)
(33) 優先権主張国 日本（ＪＰ）

(71) 出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

(72) 発明者 河田 浩嗣
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72) 発明者 勝田 昇
大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(74) 代理人 100081813
弁理士 早瀬 憲一

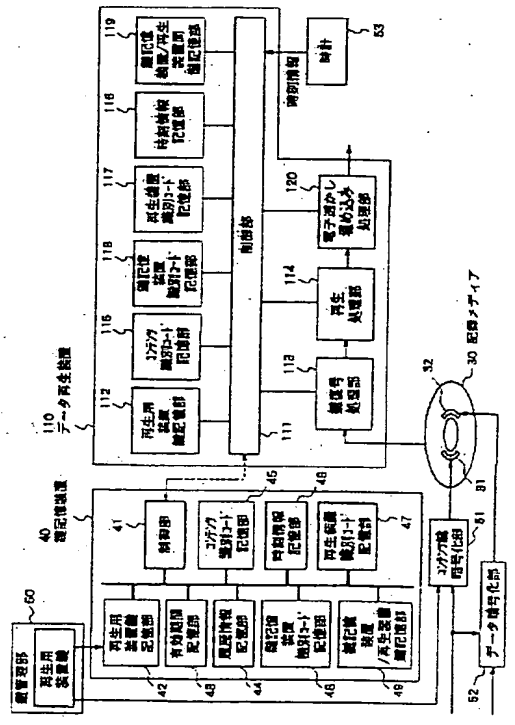
最終頁に続く

(54)【発明の名称】データ再生装置、デジタルコンテンツ再生装置、再生システム、情報埋め込み装置、及び埋め込み情報検出装置

(57)【要約】

【課題】 再生資格のないものによる不正アクセスや、時刻情報の不正操作による、不正なデータ再生を防止するデータ再生装置及び再生システム、さらに、不正コピーなど、著作物の不正使用の検知や防止を実現する情報埋め込み装置及び埋め込み情報検出装置を提供する。

【解決手段】 データ再生装置１１０ごとに作成された再生装置鍵を有する鍵記憶装置４０に、データ再生装置１１０の制御部１１１から時刻情報等を含む鍵要求コマンドを出力し、そのコマンドをうけとった鍵記憶部４０は、そのコマンドに含まれる情報から不正アクセスかどうかの確認をし、鍵読み出し履歴を記録した上で鍵をデータ再生装置１１０に配送し、その鍵を用いて復号化処理されたデータに、前記鍵読み出し履歴を電子透かし埋め込みして出力する。



1

【特許請求の範囲】

【請求項１】　復号鍵で暗号化された暗号化コンテンツを、デジタルメディアより読み出し、鍵記憶装置に記憶されている前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、

前記デジタルメディアの再生状況を監視する再生状況取得手段と、

前記復号鍵を用いて前記暗号化コンテンツを復号化するコンテンツ復号化手段とを備え、

前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツを、保持した前記復号鍵を用いて、前記コンテンツ復号化手段により復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部に保持していた前記復号鍵を破棄する、

ことを特徴とするデータ再生装置。

【請求項２】　請求項１記載のデータ再生装置において、

前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄する、

ことを特徴とするデータ再生装置。

【請求項３】　請求項1または請求項２記載のデータ再生装置において、前記デジタルメディアはＤＶＤである、ことを特徴とするデータ再生装置。

【請求項４】　コンテンツ鍵で暗号化された暗号化コンテンツと、復号鍵で暗号化された暗号化コンテンツ鍵とを、デジタルメディアより読み出し、鍵記憶装置に記憶された前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該鍵記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、

前記デジタルメディアの再生状況を監視する再生状況取得手段と、

前記復号鍵を用いて、前記暗号化コンテンツ鍵を前記コンテンツ鍵に復号化する暗号化コンテンツ鍵復号化手段と、

前記コンテンツ鍵を用いて、前記暗号化コンテンツを復号化する暗号化コンテンツ復号化手段とを備え、

前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツ鍵を、保持した前記復号鍵を用いて、前記コンテンツ鍵復号化手段により復号化して前記コンテンツ鍵を取得し、該コンテンツ鍵を用いて、前記デジタルメディアから読み出した前記暗号化コンテンツを復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部

2

に保持していた前記復号鍵を破棄する、

ことを特徴とするデータ再生装置。

【請求項５】　請求項４記載のデータ再生装置において、

前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄する、

ことを特徴とするデータ再生装置。

【請求項６】　請求項４または請求項５記載のデータ再生装置において、

前記デジタルメディアはＤＶＤである、ことを特徴とするデータ再生装置。

【請求項７】　デジタルメディアに記録されている、暗号化されたデータを復号化する復号鍵を記憶している復号鍵記憶手段と、該暗号化データを再生する際に、外部装置へ前記復号鍵の読み出し許可を与える鍵読み出し許可手段と、前記復号鍵の外部装置への読み出し実績を記録する鍵読み出し履歴記録手段とを備えた鍵記憶装置であって、

前記復号鍵は、該復号鍵の読み出し有効期間である有効期間情報を含み、

前記鍵読み出し許可手段は、前記外部装置から前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻を含む鍵要求信号を受け取り、前記鍵読み出し時刻が、前記鍵読み出し履歴記録手段により記録された前記復号鍵の鍵読み出し履歴情報のうちのもっとも新しい時刻よりも後の時刻であることと、前記鍵要求時刻が前記鍵の読み出し有効期間内にあることと、前記鍵読み出し履歴記録手段により前記鍵読み出し履歴情報が記録されたことを確認したうえで、該外部装置に前記復号鍵の読み出し許可を与えるものである、

ことを特徴とする鍵記憶装置。

【請求項８】　請求項７記載の鍵記憶装置において、

前記鍵読み出し履歴記録手段は、前記鍵読み出し履歴情報に加えて、該鍵読み出し履歴情報の改ざん検出可能な改ざん検出コードをさらに生成し記録する、

ことを特徴とする鍵記憶装置。

【請求項９】　請求項７または請求項８記載の鍵記憶装置において、

前記鍵読み出し許可手段は、前記鍵読み出し履歴情報に付け加えられた前記改ざんコードより、前記鍵読み出し履歴情報に改ざんがないことを確認し、前記外部装置に前記復号鍵の読み出し許可を与えるものである、

ことを特徴とする鍵記憶装置。

【請求項１０】　請求項７記載の鍵記憶装置において、

前記鍵読み出し履歴記録手段は、所定の記憶容量を持ち、

前記鍵読み出し許可手段は、前記鍵読み出し履歴情報が前記鍵読み出し履歴記録手段の前記記憶容量に達した時、前記復号鍵の読み出しを不許可とするものである、

ことを特徴とする鍵記憶装置。

【請求項１１】　復号鍵で暗号化されたデータを、デジタルメディアより読み出し、再生するデータ再生装置であって、暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置から該復号鍵を取得する鍵取得手段と、前記デジタルメディアから取得した暗号化されたデータを、該復号鍵を用いて復号化する復号処理手段と、前記復号化処理手段により復号化されたデータに情報を埋め込む情報埋め込み手段と、前記データ再生装置の機器識別コードを記憶する機器識別コード記憶手段とを備え、前記鍵取得手段により前記復号鍵を取得し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻及び前記データ再生装置の機器識別コードを、前記情報埋め込み手段により、埋め込み情報として前記復号化されたデータに埋め込む、

ことを特徴とするデータ再生装置。

【請求項１２】　請求項１１に記載のデータ再生装置において、

前記鍵取得手段は、前記復号鍵を記憶している鍵記憶装置の識別コードを、該鍵記憶装置から前記復号鍵と共に読み出すものであり、

前記情報埋め込み手段は、該鍵記憶装置の識別コードを前記埋め込み情報として前記復号化されたデータにさらに埋め込むものである、ことを特徴とするデータ再生装置。

【請求項１３】　請求項１１または請求項１２に記載のデータ再生装置において、

前記情報埋め込み手段は、埋め込みパターンを各映像フレーム毎への各埋め込み列に変換する埋め込み列生成手段と、該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換するものである、ことを特徴とするデータ再生装置。

【請求項１４】　請求項１３に記載のデータ再生装置において、

前記鍵取得手段は、前記鍵読み出し時刻及び前記データ再生装置の機器識別コードを含む鍵読み出し履歴信号を生成し、前記復号鍵を保持する鍵記憶装置に伝送するものである、

ことを特徴とするデータ再生装置。

【請求項１５】　復号鍵で暗号化されたデータを、デジタルメディアから読み出し、再生するデジタルコンテンツ再生装置であって、

暗号化されたデータを再生する復号鍵を記憶する鍵記憶手段と、前記鍵記憶手段から該復号鍵を読み出して再生処理するデータ再生手段とを備え、

前記データ再生手段と前記鍵記憶手段との接続は、着脱可能であって、

前記鍵記憶手段は、前記データ再生手段が前記復号鍵を読み出したとき、前記デジタルコンテンツ再生装置の機器識別コードと、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻とを含む鍵読み出し履歴情報を記録し、前記データ再生手段は、前記復再生用鍵を用いて再生される再生データに、前記鍵読み出し時刻及び前記デジタルコンテンツ再生装置の機器識別コードを埋め込み情報として埋め込むものである、

ことを特徴とするデジタルコンテンツ再生装置。

【請求項１６】　請求項１５記載のデジタルコンテンツ再生装置において、前記埋め込み情報は、各映像フレーム毎への埋め込み列に変換されて電子透かし埋め込みされ、前記埋め込み列は、各映像フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させたものである、ことを特徴とするデジタルコンテンツ再生装置。

【請求項１７】　暗号化データの復号鍵の読み出し有効期間である有効期間情報を記録し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻と該鍵読み出し時刻に最も近い以前の時刻に記録された時刻との差を鍵未使用期間として記録し、前記鍵読み出し時刻及びデータ再生装置の機器識別コードとを含む鍵読み出し履歴情報を記録し、前記復号鍵の使用を終了した時刻を鍵使用終了時刻として記録する、

ことを特徴とする鍵読み出し履歴記録方法。

【請求項１８】　埋め込みパターンを各映像フレーム毎への埋め込み列に変換する埋め込み列生成手段と、

該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、

前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、前記埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換する、

ことを特徴とする情報埋め込み装置。

【請求項１９】　現在の時刻を特定可能な実時間情報を出力する実時刻測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入力された時点の前記実時刻情報を埋め込む情報埋め込み手段とを備える、

ことを特徴とする情報埋め込み装置。

【請求項２０】　現在の物理的な位置を特定可能な実位置情報を出力する実位置測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入力された時点の前記実位置情報を埋め込む情報埋め込み手段とを備える、

ことを特徴とする情報埋め込み装置。

【請求項２１】　現在の時刻を特定可能な実時刻情報を出力する実時刻測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実時刻測定ステップから得られた実時刻情報を埋め込む、ことを特徴とする情報埋め込み方法。

【請求項２２】　現在の位置を特定可能な実位置情報を出力する実位置測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実位置測定ステップから得られた実位置情報を埋め込む、ことを特徴とする情報埋め込み方法。

【請求項２３】　埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた埋め込み列を生成する埋め込み列生成手段と、前記埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備える情報埋め込み装置によって、埋め込み情報を埋め込まれた再生データから、前記埋め込み情報を検出する埋め込み情報検出装置であって、

該埋め込み情報検出装置は、各映像フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出手段と、

前記フレーム内埋め込み情報検出手段が検出する埋め込みパターンより、短周期埋め込みビットを参照して埋め込みパターンを算出する短周期埋め込みパターン検出手段と、

長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段とを備える、

ことを特徴とする埋め込み情報検出装置。

【請求項２４】　現在の時刻を特定可能な実時刻情報、現在の位置を特定可能な実位置情報または、視聴可能なデータを再生する装置の機器識別コードのうちの少なくとも1つを埋め込み情報として埋め込んだ前記視聴可能なデータより、該埋め込み情報を検出し、前記埋め込み情報の履歴である情報埋め込み履歴データベースと、検出した前記埋め込み情報とを照合処理する、

ことを特徴とする埋め込み情報確認方法。

【請求項２５】　請求項２４記載の埋め込み情報確認方法において、

前記埋め込み情報は、暗号化されたデータを含むデジタルメディアを再生するデータ再生装置の機器識別コード、及び該暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置に、前記復号鍵の読み出し要求した時刻である鍵読み出し時刻であり、

前記埋め込み履歴データベースは、前記復号鍵の前記データ再生装置への読み出し実績を記録する鍵読み出し履歴記憶手段を回収したものである、

ことを特徴とする埋め込み情報確認方法。

【請求項２６】　データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、

前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の時刻を特定可能な実時刻情報を出力する実時刻測定手段と、前記映像／音声データに情報を埋め込む情報埋め込み手段とを備え、

前記データ再生装置が前記入力されるデータを再生した時点における前記実時刻測定手段による前記実時刻情報を埋め込む、

ことを特徴とする再生システム。

【請求項２７】　請求項２６記載の再生システムにおいて、

一台の前記実時刻測定手段と、少なくとも一台の前記データ出力装置とを備える、ことを特徴とする再生システム。

【請求項２８】　データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、

前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の位置を特定可能な実位置情報を出力する実位置測定手段と、前記実位置情報を前記映像／音声データに埋め込む情報埋め込み手段とを備え、

前記データ再生装置が前記入力されるデータを再生した時点における前記実位置測定手段による前記実位置情報を埋め込む、

ことを特徴とする再生システム。

【請求項２９】　請求項２８記載の再生システムにおいて、

一台の前記実位置測定手段と、少なくとも一台の前記データ出力装置とを備える、ことを特徴とするデジタルコンテンツ再生システム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、デジタルメディアのコンテンツが著作物である場合の不正使用の検知や防止を実現可能なデータ再生装置、再生システム、情報埋め込み装置及び埋め込み情報検出装置に関する。

【０００２】

【従来の技術】従来のデータ再生装置は、デジタルバー

サタイルディスクプレーヤ（ＤＶＤプレーヤ）などがある。これは、ＤＶＤに格納されたデータを著作権保護対策を行わないような機器で再生できないように、ディスクにかかれるデータを暗号化して記録してあり、正規に鍵を付与されたプレーヤのみ再生が可能になるものである。一般のＤＶＤプレーヤの場合、この再生に必要な鍵は、機器固定に与えられている。たとえば、図１８を用いて、従来のデータ再生装置を説明する。

【０００３】図１８は、従来のデータ再生装置の一構成例を示す図である。

【０００４】図１８において、１０００は、デジタルメディア１２００に記録されている暗号化コンテンツ１２０２を復号化する鍵であるコンテンツ鍵を記憶している鍵記憶装置、１１００はデータ再生装置である。鍵記憶装置１０００は、制御部１００１と上記コンテンツ鍵を記憶している鍵記憶部１００２が備わっている。また、データ再生装置１１００は、制御部１１０１と、鍵記憶装置１０００からコンテンツ鍵を取得し、保持するコンテンツ鍵保持部１１０２と、デジタルメディア１２００から暗号化コンテンツ１２０２を読み出す読み出し部１１０４と、その暗号化コンテンツ１２０２復号化処理する暗号化コンテンツ復号化部１１０５と、その復号化されたコンテンツを再生する再生部１１０６と、それを外部へ出力する信号出力部１１０７と、ユーザからの指示を制御部に伝えるユーザ操作入力部１１０８とからなる。

【０００５】以上のシステムからなるデータ再生装置において、ユーザからユーザ操作入力部１１０８を介して、デジタルメディア１２００のコンテンツの再生を指示された場合の動作を説明する。

【０００６】データ再生装置１１００は暗号化コンテンツ１２０２の再生に際してデータ再生装置１１００の制御部１１０１を用いて、鍵記憶装置１０００の制御部１００１と通信し、自らがデジタルメディア１２００内にある暗号化コンテンツ１２０２を再生する資格を有することを立証する。鍵記憶装置の制御部１００１によって、再生の資格を有することを認証されたら、データ再生装置１１００は、鍵記憶装置１０００よりコンテンツ鍵を取得し、コンテンツ鍵保持部１１０２に保存する。その後、データ再生装置１１００は、デジタルメディア１２００より暗号化コンテンツ１２０２を読み出し部１１０４により取得し、先ほど保存しておいたコンテンツ鍵を用いて暗号化コンテンツ１２０２を暗号化コンテンツ復号化部１１０５によって復号化し、平文コンテンツを取得する。その後データ再生装置１１００は、再生部１１０６を用いて平文コンテンツを再生処理し、信号出力部１１０７より信号を出力する。このような構成をとることで、あるデジタルメディア上に存在する特定の暗号化コンテンツの再生にあたっては、鍵記憶装置１０００によりデータ再生装置１１００がその暗号化コンテンツを再生する資格を有するかどうかの確認が取られることが必要となり、このことにより資格をもたない不正なプレーヤがデジタルメディア上の暗号化コンテンツを再生することを防ぐ効果が期待できる。

【０００７】一方、映画館の劇場への電子配信や航空機内のビデオサービスにおいては、劇場で公開される以前のものなどがあり、その再生できる期間を制御できるものが望まれている。このようなデータへのアクセスについては、特開平１０－３４１２１２号に暗号文伝送システムが開示されている。この暗号文伝送システムにおいては、鍵に有効期限または使用可能位置情報を持たせ、鍵を利用する際に現在時刻または現在位置を検出し、その時刻が有効期限内にあるか、またはその使用位置が使用可能位置内にあるかどうかによって、鍵の利用を制御することができる。さらに、定期的に時刻情報を記録し、その時刻情報と現在時刻を比較することでも、鍵の利用を制御することができる。

【０００８】また、データ内に信頼性の高い位置情報や時刻情報を埋め込む方法としては、特開２０００－５０１９３号にデジタル画像生成方法及び装置並びに記憶媒体が開示されている。このデジタル画像生成方法及び装置においては、デジタル画像データを作成している場所近傍において、ＧＰＳ衛星からの電波を受信し、この受信電波により得た画像作成時の位置情報や時刻情報を暗号化して画像再生する際に視覚的に認知不可能な深層付加情報として上記デジタル画像データに電子透かし埋め込みし、信頼性の高い十分な証拠能力を備えたデジタル画像を生成することができる。

【０００９】

【発明が解決しようとする課題】しかし、従来のデータ再生装置では、一度鍵記憶装置から、特定のコンテンツの再生資格があることが認められてコンテンツ鍵を入手し、コンテンツ鍵保持部に記憶してしまえば、本来資格のないはずの暗号化コンテンツの再生に関して、保存済みのコンテンツ鍵を用いることで不正に再生ができてしまう問題があった。

【００１０】また、特開平１０－３４１２１２号に開示されている方法では、鍵を再生装置側に送信してから、時刻情報や位置情報の判定を行うので、鍵を不正に取得される可能性があった。さらに、現在時刻の確認を行い、鍵の不正取得を防止するため記録している時刻情報を改ざんされ、鍵を不正に取得される可能性があった。

【００１１】また、特開２０００－５０１９３号に開示されている方法は、データ作成時点の信頼性の高い位置情報や時刻情報を埋め込むものであって、そのデータを復号化して再生した時点に、著作権を保護するために位置情報や時刻情報を埋め込むものではなかった。

【００１２】さらに、再生データに埋め込み情報を埋め込んだ場合、それを正しく検出する必要があるが、埋め込み情報が増えた場合、そのすべての情報を間違いなく

検出することが困難になるうえ、その検出結果が正しいかどうかを保証できる手段がなかった。

【００１３】本発明は、以上のような問題に鑑みてなされたものであり、再生資格のないものによる不正アクセスや、時刻情報の不正操作による不正なデータ再生を防止し、不正コピー等、著作物の不正使用の検知や防止を実現するデータ再生装置、デジタルコンテンツ再生装置、再生システム、情報埋め込み装置、及び埋め込み検出装置を提供することを目的とする。

【００１４】

【課題を解決するための手段】このような課題を解決するため、本発明の請求項１記載のデータ再生装置は、復号鍵で暗号化された暗号化コンテンツを、デジタルメディアより読み出し、鍵記憶装置に記憶されている前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、前記デジタルメディアの再生状況を監視する再生状況取得手段と、前記復号鍵を用いて前記暗号化コンテンツを復号化するコンテンツ復号化手段とを備え、前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツを、保持した前記復号鍵を用いて、前記コンテンツ復号化手段により復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたものである。

【００１５】また、本発明の請求項２記載のデータ再生装置は、請求項１記載のデータ再生装置において、前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたものである。

【００１６】また、本発明の請求項３記載のデータ再生装置は、請求項1または請求項２記載のデータ再生装置において、前記デジタルメディアはＤＶＤであるようにしたものである。

【００１７】また、本発明の請求項４記載のデータ再生装置は、コンテンツ鍵で暗号化された暗号化コンテンツと、復号鍵で暗号化された暗号化コンテンツ鍵とを、デジタルメディアより読み出し、鍵記憶装置に記憶された前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該鍵記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、前記デジタルメディアの再生状況を監視する再生状況取得手段と、前記復号鍵を用いて、前記暗号化コンテンツ鍵を前記コンテンツ鍵に復号化する暗号化コンテンツ鍵復号化手段と、前記コンテンツ鍵を用いて、前記暗号化コンテンツを復号化する暗号化コンテンツ復号化手段とを備え、前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツ鍵を、保持した前記復号鍵を用いて、前記コンテンツ鍵復号化手段により復号化して前記コンテンツ鍵を取得し、該コンテンツ鍵を用いて、前記デジタルメディアから読み出した前記暗号化コンテンツを復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたものである。

【００１８】また、本発明の請求項５記載のデータ再生装置は、請求項４記載のデータ再生装置において、前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたものである。

【００１９】また、本発明の請求項６記載のデータ再生装置は、請求項４または請求項５記載のデータ再生装置において、前記デジタルメディアはＤＶＤであるようにしたものである。

【００２０】また、本発明の請求項７記載の鍵記憶装置は、デジタルメディアに記録されている、暗号化されたデータを復号化する復号鍵を記憶している復号鍵記憶手段と、該暗号化データを再生する際に、外部装置へ前記復号鍵の読み出し許可を与える鍵読み出し許可手段と、前記復号鍵の外部装置への読み出し実績を記録する鍵読み出し履歴記録手段とを備えた鍵記憶装置であって、前記復号鍵は、該復号鍵の読み出し有効期間である有効期間情報を含み、前記鍵読み出し許可手段は、前記外部装置から前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻を含む鍵要求信号を受け取り、前記鍵読み出し時刻が、前記鍵読み出し履歴記録手段により記録された前記復号鍵の鍵読み出し履歴情報のうちのもっとも新しい時刻よりも後の時刻であることと、前記鍵要求時刻が前記鍵の読み出し有効期間内にあることと、前記鍵読み出し履歴記録手段により前記鍵読み出し履歴情報が記録されたこととを確認したうえで、該外部装置に前記復号鍵の読み出し許可を与えるようにしたものである。

【００２１】また、本発明の請求項８記載の鍵記憶装置は、請求項７記載の鍵記憶装置において、前記鍵読み出し履歴記録手段は、前記鍵読み出し履歴情報に加えて、該鍵読み出し履歴情報の改ざん検出可能な改ざん検出コードをさらに生成し記録するようにしたものである。

【００２２】また、本発明の請求項９記載の鍵記憶装置は、請求項７または請求項８記載の鍵記憶装置において、前記鍵読み出し許可手段は、前記鍵読み出し履歴情報に付け加えられた前記改ざんコードより、前記鍵読み出し履歴情報に改ざんがないことを確認し、前記外部装置に前記復号鍵の読み出し許可を与えるようにしたものである。

【００２３】また、本発明の請求項１０記載の鍵記憶装

置は、請求項７記載の鍵記憶装置において、前記鍵読み出し履歴記録手段は、所定の記憶容量を持ち、前記鍵読み出し許可手段は、前記鍵読み出し履歴情報が前記鍵読み出し履歴記録手段の前記記憶容量に達した時、前記復号鍵の読み出しを不許可とするようにしたものである。

【００２４】また、本発明の請求項１１記載のデータ再生装置は、復号鍵で暗号化されたデータを、デジタルメディアより読み出し、再生するデータ再生装置であって、暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置から該復号鍵を取得する鍵取得手段と、前記デジタルメディアから取得した暗号化されたデータを、該復号鍵を用いて復号化する復号処理手段と、前記復号化処理手段により復号化されたデータに情報を埋め込む情報埋め込み手段と、前記データ再生装置の機器識別コードを記憶する機器識別コード記憶手段とを備え、前記鍵取得手段により前記復号鍵を取得し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻及び前記データ再生装置の機器識別コードを、前記情報埋め込み手段により、埋め込み情報として前記復号化されたデータに埋め込むようにしたものである。

【００２５】また、本発明の請求項１２記載のデータ再生装置は、請求項１１に記載のデータ再生装置において、前記鍵取得手段は、前記復号鍵を記憶している鍵記憶装置の識別コードを、該鍵記憶装置から前記復号鍵と共に読み出すものであり、前記情報埋め込み手段は、該鍵記憶装置の識別コードを前記埋め込み情報として前記復号化されたデータにさらに埋め込むようにしたものである。

【００２６】また、本発明の請求項１３記載のデータ再生装置は、請求項１１または請求項１２に記載のデータ再生装置において、前記情報埋め込み手段は、埋め込みパターンを各映像フレーム毎への各埋め込み列に変換する埋め込み列生成手段と、該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換するようにしたものである。

【００２７】また、本発明の請求項１４記載のデータ再生装置は、請求項１３に記載のデータ再生装置において、前記鍵取得手段は、前記鍵読み出し時刻及び前記データ再生装置の機器識別コードを含む鍵読み出し履歴信号を生成し、前記復号鍵を保持する鍵記憶装置に伝送するようにしたものである。

【００２８】また、本発明の請求項１５記載のデジタルコンテンツ再生装置は、復号鍵で暗号化されたデータ

を、デジタルメディアから読み出し、再生するデジタルコンテンツ再生装置であって、暗号化されたデータを再生する復号鍵を記憶する鍵記憶手段と、前記鍵記憶手段から該復号鍵を読み出して再生処理するデータ再生手段とを備え、前記データ再生手段と前記鍵記憶手段との接続は、着脱可能であって、前記鍵記憶手段は、前記データ再生手段が前記復号鍵を読み出したとき、前記デジタルコンテンツ再生装置の機器識別コードと、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻とを含む鍵読み出し履歴情報を記録し、前記データ再生手段は、前記復再生用鍵を用いて再生される再生データに、前記鍵読み出し時刻及び前記デジタルコンテンツ再生装置の機器識別コードを埋め込み情報として埋め込むようにしたものである。

【００２９】また、本発明の請求項１６記載のデジタルコンテンツ再生装置は、請求項１５記載のデジタルコンテンツ再生装置において、前記埋め込み情報は、各映像フレーム毎への埋め込み列に変換されて電子透かし埋め込みされ、前記埋め込み列は、各映像フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させたようにしたものである。

【００３０】また、本発明の請求項１７記載の鍵読み出し履歴記録方法は、暗号化データの復号鍵の読み出し有効期間である有効期間情報を記録し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻と該鍵読み出し時刻に最も近い以前の時刻に記録された時刻との差を鍵未使用期間として記録し、前記鍵読み出し時刻及びデータ再生装置の機器識別コードとを含む鍵読み出し履歴情報を記録し、前記復号鍵の使用を終了した時刻を鍵使用終了時刻として記録するようにしたものである。

【００３１】また、本発明の請求項１８記載の情報埋め込み装置は、埋め込みパターンを各映像フレーム毎への埋め込み列に変換する埋め込み列生成手段と、該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、前記埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換するようにしたものである。

【００３２】また、本発明の請求項１９記載の情報埋め込み装置は、現在の時刻を特定可能な実時間情報を出力する実時刻測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入

力された時点の前記実時刻情報を埋め込む情報埋め込み手段とを備えるようにしたものである。

【００３３】また、本発明の請求項２０記載の情報埋め込み装置は、現在の物理的な位置を特定可能な実位置情報を出力する実位置測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入力された時点の前記実位置情報を埋め込む情報埋め込み手段とを備えるようにしたものである。

【００３４】また、本発明の請求項２１記載の情報埋め込み方法は、現在の時刻を特定可能な実時刻情報を出力する実時刻測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実時刻測定ステップから得られた実時刻情報を埋め込むようにしたものである。

【００３５】また、本発明の請求項２２記載の情報埋め込み方法は、現在の位置を特定可能な実位置情報を出力する実位置測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実位置測定ステップから得られた実位置情報を埋め込むようにしたものである。

【００３６】また、本発明の請求項２３記載の埋め込み情報検出装置は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた埋め込み列を生成する埋め込み列生成手段と、前記埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備える情報埋め込み装置によって、埋め込み情報を埋め込まれた再生データから、前記埋め込み情報を検出する埋め込み情報検出装置であって、該埋め込み情報検出装置は、各映像フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出手段と、前記フレーム内埋め込み情報検出手段が検出する埋め込みパターンより、短周期埋め込みビットを参照して埋め込みパターンを算出する短周期埋め込みパターン検出手段と、長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段とを備えるようにしたものである。

【００３７】また、本発明の請求項２４記載の埋め込み情報確認方法は、現在の時刻を特定可能な実時刻情報、現在の位置を特定可能な実位置情報または、視聴可能なデータのうちの少なくとも１つを再生する装置の機器識別コードを埋め込み情報として埋め込んだ前記視聴可能なデータより、該埋め込み情報を検出し、前記埋め込み

情報の履歴である情報埋め込み履歴データベースと、検出した前記埋め込み情報とを照合処理するようにしたものである。

【００３８】また、本発明の請求項２５記載の埋め込み情報確認方法は、請求項２４記載の埋め込み情報確認方法において、前記埋め込み情報は、暗号化されたデータを含むデジタルメディアを再生するデータ再生装置の機器識別コード、及び該暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置に、前記復号鍵の読み出し要求した時刻である鍵読み出し時刻であり、前記埋め込み履歴データベースは、前記復号鍵の前記データ再生装置への読み出し実績を記録する鍵読み出し履歴記憶手段を回収したものであるようにしたものである。

【００３９】また、本発明の請求項２６記載の再生システムは、データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の時刻を特定可能な実時刻情報を出力する実時刻測定手段と、前記映像／音声データに情報を埋め込む情報埋め込み手段とを備え、前記データ再生装置が前記入力されるデータを再生した時点における前記実時刻測定手段による前記実時刻情報を埋め込むようにしたものである。

【００４０】また、本発明の請求項２７記載の再生システムは、請求項２６記載の再生システムにおいて、一台の前記実時刻測定手段と、少なくとも一台の前記データ出力装置とを備えるようにしたものである。

【００４１】また、本発明の請求項２８記載の再生システムは、データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の位置を特定可能な実位置情報を出力する実位置測定手段と、前記実位置情報を前記映像／音声データに埋め込む情報埋め込み手段とを備え、前記データ再生装置が前記入力されるデータを再生した時点における前記実位置測定手段による前記実位置情報を埋め込むようにしたものである。

【００４２】また、本発明の請求項２９記載の再生システムは、請求項２８記載の再生システムにおいて、一台の前記実位置測定手段と、少なくとも一台の前記データ出力装置とを備えるようにしたものである。

【００４３】

【発明の実施の形態】（実施の形態１）以下、図１から図３を用いて、本発明の請求項１から請求項６に記載された実施の形態１について説明する。まず、図１を用いて、本実施の形態１におけるデータ再生装置の構成を説明する。図１は、本実施の形態１のデータ再生装置の一構成例を示す図である。図１において、１０は鍵記憶装置、１００はＤＶＤプレーヤ（データ再生装置）、２０はＤＶＤ（デジタルメディア）である。鍵記憶装置１０

には、制御部１１と、コンテンツ鍵復号鍵（復号鍵）が記憶されている鍵記憶部１２が備わっている。コンテンツ鍵復号鍵は、ＤＶＤ２０上にある暗号化コンテンツ鍵２１を復号化してコンテンツ鍵を取り出す鍵であり、制御部１１はＤＶＤプレーヤ１００と相互認証を行い、該コンテンツ鍵復号鍵を読み出す許可を与えるものである。ＤＶＤプレーヤ１００には、鍵記憶装置１０と相互認証を行い、鍵読み出し許可を受ける制御部１０１と、鍵記憶装置１０から読み出したコンテンツ鍵復号鍵を記憶しておくコンテンツ鍵復号鍵保持部１０２（鍵保持部）と、暗号化されたコンテンツ鍵を復号化する暗号化コンテンツ鍵復号化部１０３と、ＤＶＤ２０からコンテンツ等を読み出す読み出し部１０４と、暗号化されたコンテンツを復号化する暗号化コンテンツ復号化部１０５と、その復号化されたデータを再生する再生部１０６と、再生部１０６で再生されたデータを出力する信号出力部１０７と、ユーザからの指示を制御部１０１に伝えるユーザ操作入力部１０８とが備わっている。ＤＶＤ２０には、暗号化コンテンツ鍵２１と暗号化コンテンツ２２が備わっている。ＤＶＤ２０上にある暗号化コンテンツ２２は、平文コンテンツをコンテンツ鍵で暗号化したものであり、暗号化コンテンツ鍵２１は、コンテンツ鍵をコンテンツ鍵復号鍵で暗号化したものである。

【００４４】次に、図２のフローチャートに従って、ＤＶＤプレーヤ１００の再生動作を説明する。図２は、本実施の形態１におけるデータ再生装置がコンテンツを再生する場合の動作を示すフローチャートである。ここでは、例えばユーザがユーザ操作入力部１０８を介して、ＤＶＤ２０上にあるコンテンツの再生を指示した場合を考える。

【００４５】まず、ステップＳ１００において、ＤＶＤプレーヤ１００がユーザからユーザ操作入力部１０８を介して、ＤＶＤ２０のコンテンツ再生の指示を受けると、ステップＳ１０１にてＤＶＤプレーヤ１００は暗号化コンテンツ２２の再生に際し、ＤＶＤプレーヤ１００の制御部１０１を用いて、鍵記憶装置１０内の制御部１１と通信して相互認証を行い、ＤＶＤ２０内にあるコンテンツを再生する資格を有するかどうかの認証を受ける。そして、ステップＳ１０２において、鍵記憶装置１０内の制御部１１によって、再生の資格を有することが認証され、鍵記憶装置１０の鍵記憶部１２内に記憶されたコンテンツ鍵復号鍵の読み出し許可が与えられたら、ステップＳ１０４にて、ＤＶＤプレーヤ１００は鍵記憶装置１０の鍵記憶部１２よりコンテンツ鍵復号鍵を取得し、コンテンツ鍵復号鍵保持部１０２に保存する。また、ステップＳ１０１にて、鍵記憶装置１０の制御部１１により再生資格を有することを認められなかった場合、ステップＳ１０３において、コンテンツ鍵復号鍵の読み出しが許可が出されず、処理を中止する。コンテンツ鍵復号鍵を取得したＤＶＤプレーヤ１００は、その後

ステップＳ１０５において、読み出し部１０４を用いて、ＤＶＤ２０より暗号化コンテンツ鍵２１を取得し、暗号化コンテンツ鍵復号化部１０３において、コンテンツ鍵復号鍵保持部１０２に保存していたコンテンツ鍵復号鍵を用いてＤＶＤ２０より取得した暗号化コンテンツ鍵２１を復号化し、コンテンツ鍵を取得する。次にステップＳ１０６において、ＤＶＤプレーヤ１００は読み出し部１０４を用いて暗号化コンテンツ２２を取得し、先ほどコンテンツ鍵復号鍵により復号化されたコンテンツ鍵を用いて、暗号化コンテンツ復号化部１０５において暗号化コンテンツ２２を復号化し、平文コンテンツを取得する。そしてステップＳ１０７にて、ＤＶＤプレーヤ１００は取得した平文コンテンツを再生部１０６において再生し、信号出力部１０７から信号を出力する。そして、制御部１０１により再生部１０６や読み出し部１０４を制御して、ＤＶＤ２０のコンテンツを再生している間、再生部１０６はステップＳ１０８にて、ＤＶＤ２０の再生状態が変化しているかどうかを常に調べ、再生状態が変化した場合はその再生状態を制御部１０１に通知する。そして制御部１０１が、再生状態がＳＴＯＰ　ＳＴＡＴＥになったと確認した場合には、ステップＳ１０９にてコンテンツ鍵復号鍵保持部１０２に指示を出し、保持していたコンテンツ鍵復号鍵を破棄し、ステップＳ１１０にて一連の動作を終了する。ここで、再生状態のＳＴＯＰ　ＳＴＡＴＥとは、ＤＶＤプレーヤ１００の動作が停止した状態にあることをいう。また、ステップＳ１０８において、再生状態がＳＴＯＰ　ＳＴＡＴＥになったと確認されていない場合は、ステップＳ１１１においてユーザの指示があったかどうかを判断し、指示がない場合は再生状態を監視しつづけ、指示がある場合はステップＳ１１２にてその指示に従って動作する。そしてステップＳ１１２以降はステップＳ１０８に戻り、再生状態をチェックする動作から同様に繰り返す。

【００４６】以上のように動作することにより、ＤＶＤプレーヤ１００は、ＤＶＤ２０上のコンテンツの再生を開始するたびに、外部の鍵記憶装置１０の制御部１１によってＤＶＤ２０上のコンテンツの再生資格があるかどうかの認証を受けることが必要となる。

【００４７】次に、図３を用いて、鍵記憶装置１０ａとＤＶＤプレーヤ１００との間の認証において、ＤＶＤプレーヤ１００が不正プレーヤであると判断された場合について説明する。図３は、ＤＶＤプレーヤ１００が、不正プレーヤであると判断された場合の鍵記憶装置、ＤＶＤ及びＤＶＤプレーヤのブロック線図である。図３において、１０ｂは、鍵記憶装置Ｍａ１０ａとは別の鍵記憶装置Ｍｂであり、鍵記憶装置Ｍａ１０ａのコンテンツ鍵復号鍵ＫＫａと同じコンテンツ鍵復号鍵ＫＫａを内部に記憶する鍵記憶部１２ａと、ＤＶＤプレーヤ１００と相互認証を行い該コンテンツ鍵復号鍵ＫＫａの読み出し許可を与える制御部１１ｂとが備わっている。また、２３

は、ＤＶＤＤａであり、暗号化コンテンツ鍵２４及び暗号化コンテンツ２５を含み、２６は、ＤＶＤＤａ２３とは別のコンテンツを有するＤＶＤＤｂであり、コンテンツ鍵Ｋｂで暗号化された暗号化コンテンツ２８と、そのコンテンツ鍵Ｋｂを鍵記憶装置Ｍｂ１０ｂの鍵記憶部１２ａ内に記憶されたコンテンツ鍵復号鍵ＫＫａで暗号化した暗号化コンテンツ鍵２７とが備わっている。なお、上述した図１と同一のものには、同一番号を付与し、説明を省略する。

【００４８】以上のような構成をもつ、ＤＶＤプレーヤ１００、２つのＤＶＤＤａ，Ｄｂ及び鍵記憶装置Ｍａ，Ｍｂにおいて、コンテンツ鍵復号鍵ＫＫａを含む鍵記憶装置Ｍａ１０ａは、ＤＶＤＤａ２３と共に配布され、この鍵記憶装置Ｍａ１０ａは、時期がくると回収されるものであるとする。また、ＤＶＤプレーヤ１００は、上述したＤＶＤＤａ２３及び鍵記憶装置Ｍａ１０ａを用いて、ＤＶＤＤａ２３内のコンテンツ２５を再生するものである。

【００４９】ここで、ＤＶＤプレーヤ１００を用いてコピーされた海賊版ＤＶＤが発見されるなどの理由で、ＤＶＤプレーヤ１００が不正なプレーヤであると判断されたとする。そして、更に鍵記憶装置Ｍｂ１０ｂ内のコンテンツ鍵復号鍵ＫＫａを用いて暗号化されたコンテンツ鍵Ｋｂによって暗号化されたコンテンツを含むＤＶＤＤｂ２６が製造され、上記コンテンツ鍵復号鍵ＫＫａが鍵記憶装置Ｍｂ１０ｂに保存され、ＤＶＤＤｂ２６と共に配布されたとする。この鍵記憶装置Ｍｂ１０ｂは、鍵記憶装置Ｍａ１０ａと同様、時期がくれば回収されるものとする。また、鍵記憶装置Ｍｂ１０ｂ内の制御部１１ｂは、ＤＶＤプレーヤ１００を不正プレーヤと認識するように変更が加えられ、他の通常のＤＶＤプレーヤ（図示せず）には今まで通りコンテンツ鍵復号鍵ＫＫａを送信するが、不正プレーヤと判断されたＤＶＤプレーヤ１００には、コンテンツ鍵復号鍵ＫＫａを送信しないようになっている。

【００５０】以上のようにすることによって、不正なプレーヤと見なされたＤＶＤプレーヤ１００が、ＤＶＤＤｂ２６以降に製造されるＤＶＤを再生できないようにする。このように、本実施の形態１においては、鍵記憶装置１０の鍵記憶部１２から取得して、ＤＶＤプレーヤ１００のコンテンツ鍵復号鍵保持部１０２に保存したコンテンツ鍵復号鍵を、再生状態がＳＴＯＰ　ＳＴＡＴＥになった場合に破棄することと、鍵記憶装置１０とＤＶＤプレーヤとの相互認証において、不正なＤＶＤプレーヤとみなされたＤＶＤプレーヤに対しては、コンテンツ鍵復号鍵を送信しないようにすることにより、不正なＤＶＤプレーヤでは、ＤＶＤ内のコンテンツを再生することができないようにすることができる。

【００５１】なお、本実施の形態１においては暗号化コンテンツを含むデジタルメディアの例としてＤＶＤを利用する構成を示したが、他のデジタルメディアを利用する構成であっても良い。

【００５２】また、本実施の形態１においては暗号化コンテンツの復号化に際し、コンテンツ鍵復号鍵と、コンテンツ鍵の２つの鍵を必要とする構成を示したが、特に２つの鍵で暗号化する必要は無く、２つ以上の鍵で暗号化し、その内の一つ以上を装置外部の鍵記憶装置１０に持たせるような構成をとっても良いし、１つの鍵で暗号化しその鍵を外部装置である鍵記憶装置に持たせるような構成をとっても良い。

【００５３】さらに、本実施の形態１においては、ＤＶＤプレーヤ１００の再生状態がＳＴＯＰ　ＳＴＡＴＥという状態になった場合に、外部から取得した復号化鍵を破棄するような構成をとっているが、ＤＶＤ２０の再生状況の他のいずれの場合においても、その状況に応じて外部から取得した復号化鍵を破棄するような構成をとっても良い。

【００５４】（実施の形態２）以下、図４から図９を用いて、本発明の請求項７から請求項１７、請求項２３及び請求項２５に記載された実施の形態２について説明する。まず、図４を用いて本実施の形態２におけるデータ再生装置及び鍵記憶装置を含むシステムの構成を説明する。

【００５５】図４は、本発明の実施の形態２のデータ再生装置および鍵記憶装置を含むシステムの構成図である。図４におけるシステムは、データ再生装置毎の再生用装置鍵（復号鍵）を生成する鍵管理部５０、再生用装置鍵を用いてコンテンツ鍵を暗号化するコンテンツ鍵暗号化部５１、コンテンツ鍵を用いて記録メディア３０に記録するコンテンツデータを暗号化するデータ暗号化部５２、再生用装置鍵を記憶し、データ再生装置１１０にその再生用装置鍵の読み出し許可を与える鍵記憶装置４０、再生用装置鍵で暗号化されたコンテンツ鍵３１とそのコンテンツ鍵で暗号化されたコンテンツ３２を含む記録メディア３０（デジタルメディア）、鍵記憶装置４０から再生用装置鍵を読み出して記録メディア３０上に記録された暗号化コンテンツ３２の再生を行うデータ再生装置１１０、データ再生装置１１０に時刻情報を与える時計５３で構成されている。また、例えば鍵記憶装置４０は、スマートカードのようなＣＰＵつきのメモリカードで実現でき、この場合メモリカード接点とICカードリーダとが、鍵記憶装置４０とデータ再生装置１１０とを接続することになる。

【００５６】ここで、鍵記憶装置４０及びデータ再生装置１１０内部の詳細な説明をする。鍵記憶装置４０は、鍵記憶装置４０を制御する制御部４１、鍵管理部５０で作成された再生用装置鍵を記憶する再生用装置鍵記憶部４２（復号鍵記憶手段）、再生用装置鍵の有効期間を記憶する有効期間記憶部４３、鍵記憶装置４０から再生用装置鍵が読み出されるときの履歴を記録する履歴情報記

録部４４（鍵読み出し履歴記録手段）、記録メディア３０上に記録された暗号化コンテンツ３２の識別コードを記憶するコンテンツ識別コード記憶部４５、データ再生装置１１０から送られてくる時刻情報を記憶する時刻情報記録部４６、再生用装置鍵が送られるデータ再生装置１１０の識別コードを記憶する再生装置識別コード記憶部４７、鍵記憶装置４０の識別コードを記憶しておく鍵記憶装置識別コード記憶部４８、鍵記憶装置４０とデータ再生装置１１０との間の通信を暗号化して行う場合、その時の暗号化または復号化に使用する鍵を記憶する鍵記憶装置／再生装置間鍵記憶部４９からなるものである。また、データ再生装置１１０は、データ再生装置１１０を制御する制御部１１１と、鍵記憶装置４０から読み出した再生用装置鍵を記憶する再生用装置鍵記憶部１１２、記録メディア３０から暗号化されたコンテンツ鍵３１を読み出して復号化する鍵復号処理部１１３（復号鍵取得手段）、その復号化されたコンテンツ鍵を用いて、記録メディア３０に含まれる暗号化されたコンテンツデータ３２を復号化して再生する再生処理部１１４（復号処理手段）、記録メディア３０内の暗号化コンテンツ３２の識別コード記憶するコンテンツ識別コード記憶部１１５、時計５３からの時刻情報を記憶する鍵取得時刻記憶部１１６、データ再生装置の識別コードを記憶する再生装置識別コード記憶部１１７（機器識別コード記憶手段）、再生用装置鍵を読み出す鍵記憶装置４０の識別コードを記憶する鍵記憶装置識別コード記憶部１１８、鍵記憶装置４０とデータ再生装置１１０との間の通信を暗号化して行う場合に使用する鍵を記憶する鍵記憶装置／再生装置間鍵記憶部１１９、上記再生処理部１１４で再生処理された再生データに電子透かしを埋め込む電子透かし埋め込み処理部１２０（情報埋め込み手段）からなるものである。

【００５７】次に、図４、図５を用いて、データ再生装置１１０及び鍵記憶装置４０を含むシステムの、記録メディア３０に暗号化コンテンツ鍵３１及び暗号化コンテンツ３２を記録する処理動作と、その記録メディア３０の暗号化コンテンツ３２を再生する処理動作について説明する。図５は、本実施の形態２における、記録メディア３０の暗号化コンテンツ３２を再生する時の、鍵記憶装置４０及びデータ再生装置１１０を含むシステムの動作を示すフローチャート図である。

【００５８】まず、記録メディア３０内に暗号化コンテンツ鍵３１及び暗号化コンテンツ３２を記録する処理動作を説明する。鍵管理部５０は、データ再生装置１１０の再生用装置鍵を生成し、鍵記憶装置４０の再生用装置鍵記憶部４２に再生用装置鍵を記憶し、その再生用装置鍵の有効期間を有効期間記憶部４３に記録する。また、映画などのコンテンツデータを記録メディア３０に書き込む書き込み者（図示せず）へ、再生用装置鍵およびその有効期間（鍵の読み出し有効期間情報）を送り、デー

タ暗号化部５２にてコンテンツデータを暗号化するのに用いられたコンテンツ鍵を、再生用装置鍵を用いて鍵暗号化部５１において暗号化する。そして、このようにして得られた暗号化コンテンツデータ３２及び暗号化コンテンツ鍵３１は、記録メディア３０に記録される。以上のように、コンテンツデータをコンテンツ鍵で暗号化した暗号化コンテンツデータ３２とそのコンテンツ鍵を再生用装置鍵で暗号化した暗号化コンテンツ鍵３１が記録された記録メディア３０が生成される。これらの処理は、一般のＤＶＤビデオの映画タイトル等の生成において行われているため、ここでは処理の概略のみを示したが、複数のデータ再生装置へ配布可能にするために、通常は、その複数の配布先に対応する複数の再生用装置鍵を用いてコンテンツ鍵を暗号化したものを、複数記憶させておく（図示せず）。

【００５９】次に、図５のフローチャートに従って、上記のようにして得られた記録メディア３０の暗号化コンテンツデータ３２を再生する場合の鍵記憶装置４０及びデータ再生装置１１０の処理動作を説明する。記録メディア３０がデータ再生装置１１０にかけられたとき、まずステップＳ２０１において、制御部１１１は、記録メディア３０のコンテンツ識別コードを読み取り、それをコンテンツ識別コード記憶部１１５に記憶する。そして、ステップＳ２０２において、時計５３からそのときの時刻情報を取得し、鍵読み出し時刻として時刻情報記憶部１１６に記憶する。次に、ステップＳ２０３にて、先ほど時刻情報記憶部１１６に記憶した鍵読み出し時刻と、コンテンツ識別コード記憶部１１５に記憶されているコンテンツ識別コードと、再生装置識別コード記憶部１１７に記憶されているデータ再生装置１１０の再生装置識別コード（データ再生装置の機器識別コード）とを、再生用装置鍵を要求する信号である鍵リクエストコマンドにつけて、接続された鍵記憶装置４０の制御部４１に送信する。このデータ再生装置１１０の制御部１１１と鍵記憶装置４０の制御部４１との間の送信データは、鍵記憶装置／再生装置間鍵記憶部４９及び１１９に記憶された、両装置で共有している鍵記憶装置／再生装置間鍵で暗号化され、通信される。また、この暗号復号化処理は、制御部４１及び１１１において、ソフト的に行うことが可能である。次に、鍵記憶装置４０の制御部４１は、データ再生装置１１０から送られてきた鍵読み出し時刻、コンテンツ識別コード、及び再生装置識別コードを、鍵記憶装置４０の時刻情報記憶部４６、コンテンツ識別コード記憶部４５、再生装置識別コード記憶部４７にそれぞれ記憶し、ステップＳ２０４において、履歴情報記憶部４４にすでに記憶されている最新の時刻と、時刻情報記憶部４６に記憶されている鍵読み出し時刻とを比較し、鍵読み出し時刻が、最新の時刻よりも以後の時刻を示していれば処理が成功し、そうでなければ、ステップＳ２０５において、データ再生装置１１０

に処理中止メッセージを発行する等して、記録メディア３０の再生処理を直ちに中止する。

【００６０】次に、ステップＳ２０６において、制御部４１は、上記鍵読み出し時刻が、有効期間記憶部４３に記憶されている再生用装置鍵の有効期間内にあるかどうかを確認し、有効期間内にあれば処理が成功したとし、そうでなければ、上述したステップＳ２０５に戻り、再生処理を直ちに中止する。そして、ステップＳ２０７において、鍵記憶装置４０の時刻情報記憶部４６、コンテンツ識別コード記憶部４５、再生装置識別コード記憶部４７に記憶されている情報を履歴情報として、履歴情報記憶部４４に記録する。ただし、これらの情報の書き込みに失敗すれば、ステップＳ２０５に戻り、再生処理を直ちに中止する。

【００６１】以上のステップＳ２０４，Ｓ２０６，Ｓ２０７における３つの処理が成功すれば、ステップＳ２０８において、鍵記憶装置４０の制御部４１は、再生用装置鍵記憶部４２に記憶されている再生用装置鍵を、鍵記憶装置識別コード記憶部４８内の鍵記憶装置４０の鍵記憶装置識別コードと共に、データ再生装置１１０の制御部１１１に送信し、ステップＳ２０９にて、制御部１１１は、鍵記憶装置４０から再生用装置鍵を取得し、その再生用装置鍵を再生用装置鍵記憶部１１２に、鍵記憶装置４０の鍵記憶装置識別コードを鍵記憶装置識別コード記憶部１１８に記憶する。

【００６２】以上のようにして、再生用装置鍵を鍵記憶装置４０から取得した後、この再生用装置鍵を鍵復号処理部１１３に入力し、ステップＳ２１０で制御部１１１が記録メディア３０より暗号化コンテンツ鍵３１を読み出し、ステップＳ２１１において復号化してコンテンツ鍵を取得する。このコンテンツ鍵を再生処理部１１４に入力し、ステップＳ２１２において、制御部１１１が記録メディア３０から暗号化コンテンツデータ３２を読み出し、上記コンテンツ鍵を用いて復号化した後、ステップＳ２１３にてそのデータの内容にしたがって再生処理する。このデータの内容にしたがった再生処理とは、たとえば、ＭＰＥＧ２フォーマットで圧縮されたビデオデータの場合、ＭＰＥＧ２デコーダ処理し、映像信号に再生するということである。そして、ステップＳ２１４において、データ再生装置１１０の再生装置識別コード記憶部１１７、鍵記憶装置識別コード記憶部１１８、時刻情報記憶部１１６にそれぞれ記憶されている、再生装置識別コード、鍵記憶装置識別コード、または再生用装置鍵を読み出し要求した時刻である鍵読み出し時刻を埋め込み情報とし、電子透かし埋め込み処理部１２０において、再生処理部１１４から出力された再生データに上記埋め込み情報を電子透かし埋め込みし、データ再生装置１１０外部に出力する。

【００６３】そして、再生処理部１１４において記録メディア３０のコンテンツデータの再生処理が終了した後、ステップＳ２１５にて、データ再生装置１１０の制御部１１１は、鍵使用終了時に、時計５３から終了した時刻である鍵使用終了時刻を鍵記憶装置４０の制御部４１に送信し、ステップＳ２１６において、鍵記憶装置４０の制御部４１は、上記鍵使用終了時刻を履歴情報記憶部４４に記録し、再生処理が終了する。

【００６４】ここで、図６及び図７を用いて、図５におけるステップＳ２０７及びステップＳ２１６で記述した履歴情報記入について、詳しく説明する。図６は、本実施の形態２における履歴情報の記録例であり、図７は、その履歴情報の記録処理を示したフローチャート図である。なお、図６の最初の1行目は、すでに書き込まれているもので、ここには鍵の有効期間の開始時刻が書き込まれている。

【００６５】まず、その時点で書き込まれている最終行の次の行の１列目に、ステップＳ３０２において、上記最終行の一番左の列の時刻情報と、時刻情報記憶部４６に記憶されている再生用装置鍵を要求した時刻である鍵読み出し時刻との時間差を未使用時間として記録し、同行の２列目には、上記最終行の一番左の列の時刻情報を、３列目は、上記鍵読み出し時刻を記録する。そして、今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する未使用時刻記録処理を行う。

【００６６】次に、ステップＳ３０２の未使用時刻記録処理で書き込んだ次の行に、ステップＳ３０３において、上記鍵読み出し時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録する開始時刻記録処理を行う。

【００６７】そして、図５のステップＳ２１５、Ｓ２１６で説明したように、データ再生装置１１０の制御部１１１が再生用装置鍵の使用を終了したことを示す信号として、時計５３から取得した時刻情報を鍵記憶装置４０に送信したとき、鍵記憶装置４０の制御部４１は、その時刻情報を受け取り、ステップＳ３０４にて、先ほどのステップＳ３０３の開始時刻記録処理で書き込んだ次の行に、鍵使用終了時刻記憶処理を行う。これは、データ再生装置１１０から送られてきた鍵使用終了時刻を1列目に、2列目に再生装置識別コード、3列目にコンテンツ識別コードを記録し、さらに今書き込んだ行と一つ前の行のデータについての改ざん検出用のハッシュ処理を行い4列目に記録するものである。

【００６８】以上の処理により、履歴情報は、常に記録されるたびに直前の情報との改ざん検出コードでつながれるため、改ざん検出コードの生成方法が暴露されない限り、途中に不正な履歴を挟むと簡単にその位置が検出できる。そして記録されるデータの最終行の1列めデータが最新の時刻情報であり、常にこの時刻よりも進んだ

時刻が示されない限り、図５のステップＳ２０４で説明したように、処理が中止されて鍵配送されなくなるので、時刻情報を逆に進ませる不正を防止できる。

【００６９】また、履歴情報に再生用装置鍵の読み出し時刻に加えて鍵使用終了時刻をも記録した場合には、少なくともその再生時間分は時計５３の時刻を進ませることができる。

【００７０】さらに、鍵記憶装置４０の履歴情報記憶部４４の容量を有限の値にしておけば、その記憶容量いっぱいに履歴が書き込まれると、それ以上履歴が書き込めないので、図５のステップＳ２０７で説明したように処理が不成功となり鍵配送されなくなるため、記憶容量によって鍵取得回数の上限を制限できる。

【００７１】次に、図８から図１０を用いて、図５におけるステップＳ２１４で記述した電子透かし埋め込み方法及び、その埋め込んだ埋め込み情報の検出方法について、詳しく説明する。図８は、電子透かし情報埋め込み処理部１２０の構成とその検出装置の構成の説明図であり、図９は、埋め込み処理の結果、各フレームに埋め込まれるパターン列を説明した図であり、図１０は、図６のように記録された履歴を電子透かし情報の読み出し処理に利用する場合の説明図である。

【００７２】まず、図８を用いて、本実施の形態２における電子透かし埋め込み処理部１２０の構成について説明する。図８において、埋め込みシーケンス生成部１２１は、埋め込み情報を各映像フレームに埋め込むパターン列に変換するものであり、電子透かし埋め込み処理部１２２は、埋め込みシーケンス１２１によって作成されたパターン列を各フレーム毎に情報埋め込み処理し、入力されるデータを埋め込み情報つきデータとするものである。また、電子透かし検出部１２５は、電子透かし埋め込み処理部１２２によって埋め込まれた各フレームの埋め込みパターンを検出するものであり、電子透かし短周期埋め込みパターン検出部１２３及び、長周期埋め込みパターン検出部１２４は、電子透かし検出部１２５で検出された埋め込みパターンから埋め込み情報を検出するものである。

【００７３】以上の構成において、図８及び図９を用いて以下にその動作を説明する。埋め込みパターンとして、データ再生装置１１０の機器識別コード、鍵記憶装置４０の識別コードや時刻情報を含んだビットパターンが代入される。入力されたビットパターンは、埋め込みシーケンス生成部１２１で各映像フレームに埋め込むパターンの列に変換され、各フレーム毎に電子透かし埋め込み処理部１２２に送られる。埋め込みシーケンス生成部１２１では、入力された埋め込みパターンを１フレーム当たりに埋め込めるビット数に応じて分割して各フレームへの埋め込みパターンとする。例えば簡単のため、ここでは図９に示すように、埋め込みパターンが８バイトで１フレーム当たり４ビット埋め込み処理する場合、

埋め込みパターンが“０１１００１０１１１００１０１０”ならば、各フレームには、順に１６進数で“６５ｃａ”を最初の４フレームに埋め込む。次に、今の埋め込みパターンと同じフレーム数に埋め込みパターンの第１ビット値である“０”を入力する。つまり、先程入れたパターンと同じフレーム長の間、埋め込みパターンの先頭ビット値を埋め込み値として埋め込む。例えば、埋め込み値が０のときは、４フレーム間０を、１の場合は、４フレーム間１６進数でＦＦＦＦを出力する。次に再び最初に埋め込んだパターン“６５ｃａ”を順に埋め込み、次に埋め込みパターンの第２のビット値を埋め込む。以上のように、埋め込みパターンを順に埋め込み、次にそれと同じ長さの期間内に、埋め込みパターンの１ビットだけ埋め込むことを順に繰り返す。すなわち、順に埋め込んだ短周期の埋め込みとそのビット数倍の長周期に繰り返す埋め込みパターン列を生成する。

【００７４】検出の場合は、電子透かし情報検出部１２５で各フレーム毎の埋め込みパターンを検出する。本実施の形態２では、原画像を参照画像として用いているが、参照画像なしで検出できる埋め込み方式の場合は、原画像を参照しなくてもよい。各フレームの埋め込みパターン検出結果は、短周期埋め込みパターン検出部１２３、長周期埋め込みパターン検出部１２４へ送られる。短周期埋め込みパターン検出部１２３は、短周期に埋め込まれたビット列部分の検出結果を繰り返し比較し、各ビットで最も出現回数が多い方のビット値として検出値とする。長周期埋め込みパターン検出部１２４は、各ビットの埋め込み期間内での検出結果、たとえば、図９における第５フレームから第８フレームまでが、すべて１かあるいは０であるかを検出する。検出した値がすべて同じでない場合、より多くのビット値を示す側の値とする。

【００７５】上述した短周期及び長周期処理を使用した埋め込みパターンでは、短周期埋め込みパターン検出により、わずかなフレームで埋め込み情報が解読できる。また、長周期埋め込みパターン検出により、長周期的に１ビットずつ検出するため、少しの電子透かしを改ざんしても多数決判定することで、正しい値を求めることができ、各ビットの判定を埋め込みパターン分判定することで埋め込みパターンを求めることができる。

【００７６】短周期で埋め込んだ場合、映像中の数フレーム毎に埋め込み情報があるため、映像データを編集されたりしても検出できるが、フレームを抜き取るなどの改ざんに弱い。一方、長周期に埋め込んだ場合、長い期間の映像データを検出しないと埋め込みパターンが検出できないが、フレームを抜き取るなどの攻撃に強い。このように、上記２つの埋め込みパターンを併用することで弱点を補いあった、改ざんや編集につよい埋め込み方法が実現できる。

【００７７】なお、長周期と短周期の併用の仕方である

が、本実施の形態２における例以外のやり方でも同様の効果が期待できる。たとえば、１フレームに４ビット埋め込むとしてそのうち３ビットを短周期の埋め込み用に、１ビットを長周期の埋め込み用に用いて、両方を並列に埋め込むこともできる。

【００７８】次に、図１０を用いて、図６のように記録された履歴情報を、上述したような、埋め込み情報の読み出し処理に利用する場合について説明する。図１０は、不正機器、不正鍵記録装置または不正を行った時刻の特定をする場合の装置構成例を示す図である。図１０において、６０は、不正に複製された記録メディアであり、１３１は、電子透かし情報検出装置で、例えば図７の電子透かし検出部１２５、短周期埋め込みパターン検出部１２３及び長周期埋め込みパターン検出部１２４からなるものである。１３２は、データ再生装置１１０の再生装置識別コードによる検索検証処理、１３３は、鍵記憶装置４０の鍵記憶装置識別コードによる検索検証処理、１３４は、鍵読み出し時刻情報による検索検証処理である。

【００７９】電子透かし情報検出処理１３１で検出された埋め込み情報は、不正者により改ざんされている可能性がある。すなわち、不正を働いた者は、埋め込み情報による追跡から逃れるために、埋め込み情報の削除や改ざんを試みることが想定される。その結果、埋め込み部分を抜き取ることによる情報の欠損や、でたらめなデータの埋め込みによる改ざんによる、一部のデータの誤検出が考えられる。そこで、埋め込まれた情報のどれか一つでも正しく検出されていた場合には、鍵記憶装置４０の履歴情報記憶部４４に貯えられた履歴を回収した履歴データベースを検索することで、残りの情報を復元できる。つまり、再生装置識別コードによる検索検証処理１３２、鍵記憶装置識別コードによる検証処理１３３、鍵読み出し時刻情報による検証処理１３４において、それぞれの情報から残りの情報を復元できる。またこれらの情報をまとめて、それと最も相関性の高いものを履歴情報から見つけることでも、かなり高い確率で不正を行ったデータ再生装置や鍵記憶装置や犯行時刻等が推定できる。

【００８０】以上に示したように、本実施の形態２のデータ再生装置１１０によれば、鍵記憶装置４０にその再生用装置鍵の読み取り履歴を記録しているため、有効期限確認等で現在の時刻を偽って申告しようと試みた場合でも、かならず時計を進める方向にしか再生用装置鍵を受け取れる時刻はないので、不正が出来たとしても高々常に再生しつづけた場合に再生できる再生時間以上に再生させることが出来ないように出来る。

【００８１】また、鍵記憶装置４０の履歴情報記憶部４４の容量は有限なので、履歴容量を越えて鍵を取得することはできず、不正回数の上限を制限できる。また、履歴についてもハッシュ値をつけることにより改ざんが困

難な履歴書き込みが実現できる。

【００８２】さらに、本実施の形態２によれば、鍵記憶装置４０の履歴情報記憶部４４に記録した履歴情報で埋め込みデータの検出精度をあげることができ、また、上記履歴情報と埋め込み情報で検出した結果との照合は、より確かな不正の証拠を示すことが出来る。さらに情報埋め込みパターンとして短周期と長周期に２つの方法を併用して埋め込むため、改ざんに強い埋め込み方法が実現できる。

【００８３】なお、本実施の形態２においては、鍵記憶装置４０が鍵の読み出しの際、鍵の有効期間などのチェックを行ったが、データ再生装置１１０の耐タンパ性が保証されていて改造されないのであれば、データ再生装置１１０が、鍵記憶装置４０から鍵情報や履歴情報を暗号通信で受け取り、それに基づきデータ再生装置側で有効期間等の判定をさせる構成をとることも出来る。この場合は、履歴情報もデータ再生装置側で作成し、鍵記憶装置４０に暗号通信して記録させることもできる。

【００８４】また、図５のステップＳ２０４の前回アクセス時刻チェックにおいて、履歴情報から時刻情報を取り出す際、図６のハッシュ値を用いて履歴データ自身が改ざんされていないかどうか確認させると、より安全性が向上する。すなわち履歴情報中からハッシュ値を計算した場合と同じ処理をしてハッシュ値との一致を調べることで改ざんチェックが実現できる。

【００８５】また、本実施の形態２では、履歴情報記入に際して、再生用装置鍵の読み出し要求時の時刻、使用終了時の時刻、不使用の時刻と完全に連続した履歴を記録したが、単に、鍵へのアクセス時刻のみを記録しても時計を進ませる方向にしか動かせられない特徴は維持でき、本発明の効果を維持しているものである。

【００８６】（実施の形態３）以下、図１１及び図１２を用いて、本発明の請求項１９から請求項２２及び請求項２４に記載された実施の形態３について説明する。まず、図１１を用いて、映像／音声信号に情報を埋め込む処理について説明する。図１１は、本発明の実施の形態３の情報埋め込み装置を示す構成図である。図１１において、２２０は情報埋め込み手段、２２１は実時刻測定手段、２２２は実位置測定手段、２２３はＩＤ記憶手段である。

【００８７】以上のように構成された情報埋め込み装置において、その動作を説明する。情報埋め込み手段２２０は、ＩＤ記憶手段２２３より出力される、機器を特定可能な情報であるＩＤ情報と、実時刻測定手段２２１より出力される、現在の時刻を特定可能な情報である実時刻情報と、実位置測定手段２２２より出力される、現在の物理的位置を特定可能な情報である実位置情報を、情報埋め込み手段２２０に入力される映像／音声信号に埋め込んだ後出力するものである。そして、情報埋め込み手段２２０に入力される映像／音声信号は、アナログあ

るいはディジタルの映像あるいは音声信号であり、視聴可能な状態の信号である。

【００８８】ここで、それぞれの構成要素の機能を更に詳細に説明する。実時刻測定手段２２１としては、現在の時刻を特定する情報である実時刻情報を出力可能な任意の構成の手段を用いることができる。例えば、時計やカウンタなどによって実現される。実時刻情報としては、グリニッジ標準時（イギリスの標準時刻）の年月日および時分を出力すれば良い。もちろんこれに限られず、任意の国の標準時を選択可能である。また、年月日、年月、年月日と時、あるいは年月日と時分秒など、要求や用途に応じてその表現範囲を選択可能である。また、実時刻情報は上記のような一般的な時刻を表す情報に限定されず、情報が埋め込まれた時刻を特定可能な任意の情報を用いることができる。例えば、ある特定の日時（例えば２０００年１月１日０時０分）を基準として、そこから何分後か、あるいは何時間後かなどを示す情報で表現しても良い。あるいは、電子映画館など処理（この場合は再生処理）履歴を記録可能なシステムに適用される場合には、その処理回数により表現しても良い。

【００８９】次に、実位置測定手段２２２は、ＧＰＳ（グローバル・ポジショニング・システム）に従う例に代表される、自分の物理的な位置を計測し、その位置を特定する情報である実位置情報を出力可能な任意の構成の手段である。実位置情報としては、緯度・経度の組合わせなど、物理的な位置を特定可能な任意の形態の情報を用いることができる。

【００９０】実位置測定手段２２２の実現例としては、受信した位置参照信号を元にして自分の物理的な位置を計測し、実位置情報として出力する方法がある。この例としては多くの方法が実現されている。最も代表的な実現例としては、ＧＰＳに従うものがある。ＧＰＳは、受信した複数の航法用人工衛星からの電波をアンテナで受信し、実位置測定手段が電波の到達時間からその距離を計算し、人工衛星の距離から自分の位置を測定するものである。ＧＰＳは既に自動車のナビゲーションシステムなどに実用化されている技術である。また、他の例としては、ＧＰＳと同じ原理を用いた、ＧＬＯＮＡＳＳ（グローバル・ナビゲーション・サテライト・システム）に従うものがある。また、他の例としては、ＤＧＰＳ（ディファレンシャル・ＧＰＳ）に従うものがある。ＤＧＰＳは、ＧＰＳの動作に加えて、ＦＭ電波によりＧＰＳの補正情報を受信し、ＧＰＳによる位置の補正を行うものである。また、他の例としては、ＰＨＳ（パーソナル・ハンディホン・システム）測位に従うものがある。ＰＨＳ測位は、電波の強い上位３つのＰＨＳの基地局からの電波を受信し、基地局の位置とその受信した信号の電界強度から自分の位置を測定するものである。

【００９１】実位置測定手段２２２は、上記の例で示したいずれか、あるいは組み合わせに実現可能であるが、もちろん、これらに限られるものではない。また、実位置測定手段２２２は、複数の人工衛星や固定局からアンテナによって受信した信号を、自分の物理的な位置を計測するための位置参照信号とし、位置参照信号から自分の物理的な位置を計測する任意の構成により実現可能である。その計測の方法としては、外部からの電波の到達時間や強度から自分の位置を計算する任意の手段がある。さらに、別途放送受信した補正データや、実位置測定手段２２２が搭載された車や航空機などの移動体の移動距離や移動方向などの情報や、地図などを用いてより正確な自分の位置を得る手段を組合わせても良い。あるいは、サーバから直接位置情報を得る手段や、これらの手段を組み合わせたものなど、自分の物理的な位置を測定する任意の手段をとることができる。

【００９２】情報埋め込み手段２２０は、映像／音声信号にＩＤ情報と実時刻情報と実位置情報を埋め込む任意の構成の手段である。情報の埋め込み方法は、情報を埋め込み、その後に検出可能な任意の方法により実現可能である。例えば、復号化手段２３０から出力される信号が映像信号の場合には、そのブランキング期間に多重する方法がある。あるいは、電子透かしあるいはウォーターマークとして知られる画像あるいは音声中に情報を埋め込む任意の手段を用いることができる。

【００９３】ここで、電子透かしによる情報埋め込みの例を下記に示す。電子透かしによる情報埋め込みの方法として、埋め込む情報に対応する画素の画素置換を用いることができる。この方法によれば、まず、埋め込む情報に基づいて、映像の各フレームから一つ以上の画素を選択する。選択の方法としては、例えば、情報より数字を算出し、その数字が示す位置の画素を選ぶ方法がある。次に、選択された画素の情報を隣接画素の情報から算出された情報によって置換する。情報の検出の際には、情報が埋め込まれた画像と情報が埋め込まれていない画像、すなわちストリームから復号化された原画像を比較することにより、どの画素が置換されているかを検出可能であり、その検出された画素の位置から情報を復元可能である。

【００９４】電子透かしの他の例としては、例えば、日経エレクトロニクスの1997年２月24日号（ＮＯ．683）の149ｐ～162ｐの「電子透かしを支えるデータハイディング技術（上）」（及びW.Bender ,D.Gruhl,N.Morimoto,A.Lu. "Techniques for data hiding" ,IBM Systems Journal,Vol 35,NOS 3&4,1996）に紹介されている方法がある。これは、擬似乱数により映像から２点の画素（Ａｉ、Ｂｉ）を選び、埋め込むビットが１のときは、Ａｉの輝度レベルＹａｉをｄだけ上げ、Ｂｉの輝度レベルＹｂｉをｄだけ下げる。逆に、埋め込むビットが０の時は、Ａｉの輝度レベルをｄだけ下げ、Ｂｉの輝度レベルをｄだけ上げる。ｄの値は１～５の間の整数とする。

これらの処理をｎ回（ｎは通常１万程度）繰り返すことにより、映像に情報を埋め込む。情報を検出する場合には、擬似乱数により映像から情報埋込時と同じ位置の２点の輝度レベル、即ち（Ｙａｉ＋ｄ、Ｙｂｉ－ｄ）又は（Ｙａｉ－ｄ、Ｙｂｉ＋ｄ）を抽出する。そしてこれら２点の差を計算する。これらの処理を夫々の位置についてｎ回繰り返し、これらの差の平均を求め、＋２ｄあるいは－２ｄのいずれにより近いかによって埋め込まれているビットが０か１かを判定する。上記以外にも、情報を埋め込む手段については、数多くの方法が知られており、任意の手段を用いることができる。

【００９５】次に、図１２を用いて、埋め込まれた情報の検出処理について説明する。図１２は、埋め込まれた情報を検出し、不正を行ったデータ再生装置や操作者を特定する例を示したブロック線図である。情報埋め込み手段２２０で映像／音声信号に埋めこまれた情報は、映像／音声信号が不正に使用された場合に、その情報埋め込み手段２２０を含む不正を行った機器やその操作者を特定する目的で用いられる。ここで、不正な使用とは、機器で再生された映像／音声信号を、許可を受けずにコピー、再送信や編集などに用いることである。

【００９６】図１２において、２８０は情報検出手段、２８１は照合手段、２８２はデータベースである。情報検出手段２８０は、映像／音声信号に埋め込まれたＩＤ情報、実時刻情報、実位置情報のうち一つ以上を検出し、出力するものであり、情報検出手段２８０における検出処理は、例えば、入力された映像／音声信号を、情報が埋め込まれる前の映像／音声信号との比較により求められた差分情報から、情報埋め込み手段２２０における埋め込み手段によって埋め込まれた情報を検出する。検出方法としては、上記に限られず、情報埋め込み手段２２０における埋め込み処理に対応した任意の方法で検出可能である。例えば、ブランキング期間に情報が埋め込まれた映像信号からは、直接情報を検出できる。また、電子透かしにより情報が埋め込まれた後の映像／音声信号は、埋め込まれる前の映像／音声信号を比較することにより、埋め込まれた情報を検出可能である。検出されたこれらの情報により、そのとき再生に用いられた機器のＩＤ情報、及び再生が行われた時刻、物理的な位置を知ることができる。これらの情報は、不正使用された映像／音声信号から、不正が行われた機器や操作者を調査するための情報として用いることが可能である。

【００９７】さらに、データベース２８２に、機器を操作した操作者ＩＤと、その操作した機器のＩＤ情報、操作した時刻、操作した場所などの対応を記録しておけば、照合装置２８１によって、操作者ＩＤの特定ができる。このようなデータベースは、例えば、電子映画館や航空機内のＡＶシステムなどの操作者が特定可能なシステムにおいて、各データ再生装置の管理者からの報告などによって、作成可能である。なお、データベース２８２及び照合手段２８１は、データベース２８２を構築できるようなシステムにおいては、より簡単に操作者を特定できる効果がある。

【００９８】以上示したように、本実施の形態３における情報埋め込み装置によれば、情報埋め込み装置単体、あるいは映像／音声信号のデータ再生装置や記録装置、編集装置などに実装、あるいは同時に使用することにより、映像／音声信号が不正に処理された場合に、その不正な使用の検知、すなわち不正に使用された機器、時刻、位置を特定することが可能である。例えば、あるデータ再生装置に本実施の形態３の情報埋め込み装置２２０を実装し、データ再生装置の再生信号に情報を埋め込むように使用する場合を考える。この場合、データ再生装置から再生された映像／音声信号が不正に記録媒体に記録された場合に、その記録された映像／音声信号から、再生が行われた機器、時刻、位置などを特定することが可能である。これにより、不正者を特定し、さらなる不正の防止が期待できる。

【００９９】さらに、本実施の形態３によれば、不正をした者を特定可能な情報も検出可能であるので、不正をしようとする者に対する抑止効果も期待できる。なお、本実施の形態３では、ＩＤ情報、実時刻情報、実位置情報を多重するとしたが、たとえば、実位置測定手段２２２が無く、ＩＤ情報と実時刻情報のみを多重するような構成でも良い。この場合、再生が行われた機器と時刻を検出可能であるという効果が得られる。あるいは、実時刻測定手段２２１が無く、ＩＤ情報と実位置情報を多重する、あるいは実位置情報のみを多重するような構成でも良い。この場合、再生が行われた機器と位置、あるいは位置のみを検出可能であるという効果が得られる。

また、本実施の形態３では、映像／音声信号を処理の対象としているが、映像のみ、音声のみを処理の対象としても良い。あるいは、ＭＰＥＧなどで圧縮された映像あるいは音声を処理の対象としても良い。さらには、文書やプログラムなどのデータを処理の対象としてもよく、同様の効果が得られる。なお、ＩＤ記憶手段２２３はＩＣカードなどの着脱可能な装置により実現されていても良く、同様の効果が得られる。

【０１００】また、本実施の形態３では、ＩＤ情報として、機器を特定できる情報を用いるような構成としたが、たとえば、ＩＤ情報として、機器の製造メーカや機器を使用する事業者、機器が使用されている航空機やバスなどの移動体や、機器が使用されているホールや映画館など、機器に関する事業者や場所を特定できる情報を用いても良い。この場合、これらの機器に関する事業者や場所を特定可能である。あるいは、ＩＤ情報として、機器を使用する者のユーザＩＤを用いても良い。ユーザＩＤは、ＩＤ記憶手段２２３に記憶されていても良いし、ＩＤ記録手段２２３の代わりにキーボードやリモコンなどの入力手段から入力されても良い。以上のよう

に、ＩＤ情報としては、機器、機器に関する事業者や場所、機器を使用するユーザなど、任意の識別情報を用いても良く、同様の効果が得られる。もちろん、これらの組み合わせによって実現しても良い。

【０１０１】なお、本実施の形態３の情報埋め込み装置は、ＩＤ情報と実時刻情報と実位置情報を埋め込むとしたが、たとえば、これらの情報以外にも、その処理が行われた機器、人、場所、会社などの特定につながるような任意の情報を埋め込むような構成にしても良く、同様の効果が得られる。

【０１０２】なお、本実施の形態３の情報埋め込み装置は、図１１に示したような構成としたが、同様の動作を行う任意の構成により実現可能である。もちろん、ＩＤ情報と実位置情報と実時刻情報の全て、あるいはいくつかを、映像／音声信号に埋め込むような処理を実現するＣＰＵやプロセッサとプログラムの組合わせでも実現可能であり、同様の効果が得られる。

【０１０３】また、ＩＤ情報や実時刻情報や実位置情報を暗号化して埋め込み、検出時に復号化するような構成とすれば、これらの情報の改ざんが困難であるという効果が得られる。また、認証や署名などの任意の暗号技術の適用により、改ざんを困難にすることもできる。

【０１０４】（実施の形態４）以下、図１３及び図１４を用いて、本発明の請求項２６と請求項２８に記載された実施の形態４について説明する。図１３は、本実施の形態４の再生システムを示す構成図である。図１３において、２００はデータ再生装置、２２０は情報埋め込み手段、２１０はデータ再生装置２００を制御する制御手段、２２１は実時刻測定手段、２２２は実位置測定手段、２４０はストリーム送出装置（データ出力手段）、２３０はストリーム送出装置２４０から出力されたデータを復号化する復号化手段である。

【０１０５】ストリーム送出装置２４０は、記録媒体に記録、あるいは放送により受信した、ＭＰＥＧ－ＴＳ（ムービング・ピクチャ・エキスパート・グループ　トランスポート・ストリーム）のようなストリームを出力する装置である。また、このストリームは暗号化されており、暗号化に用いられた鍵は暗号化された状態でストリームに多重されている。なお、本実施の形態４において、情報埋め込み手段２２０、実時刻測定手段２２１、実位置測定手段２２２は、実施の形態３の各装置と同様の動作を行うため、説明を省略する。

【０１０６】以上のように構成された再生システムにおいて、その動作を説明する。ストリーム送出装置２４０から出力されたストリームは、データ再生装置２００に入力され、復号化手段２３０によって復号化される。復号化手段２３０においては、ストリームに多重されている暗号化された鍵を出力する。暗号化された鍵は、制御手段２１０によって復号され、再び復号化手段２１０に入力される。復号化手段２１０は入力した鍵によってストリームを復号化する。復号化手段２３０は、さらにストリームを視聴可能な信号に復号化する処理を行う。すなわち、多重されたストリームに対してはその分離を行い、さらに圧縮されたストリームに対してはその伸長を行い、視聴可能な信号に変換する。

【０１０７】復号化手段２３０より出力された信号は、情報埋め込み手段２２０に入力される。情報埋め込み手段２２０では、制御手段２１０より出力されるＩＤ情報と、実時刻測定手段２２１より出力される実時刻情報と、実位置測定手段２２２より出力される実位置情報が、情報埋め込み手段２２０に入力された信号に埋め込まれた後、出力される。ここで、ＩＤ情報はそのデータ再生装置２００を特定する機器に固有のＩＤである。

【０１０８】以上の構成により、データ再生装置２００によって再生された信号には、機器を特定するＩＤ情報と、再生された時刻を特定する実時間情報と、再生された場所を特定する実位置情報が埋め込まれており、またこれらの情報は検出可能なものである。したがって、データ再生装置２００によって再生された信号を許可なく記録した記録媒体を不正に販売あるいは流通した場合、その記録媒体に記録された信号から不正が行われた機器、時刻、場所を特定することが可能であるという効果が得られる。

【０１０９】よって、この特定された機器、時刻、場所の情報を利用すれば、さらなる不正を防ぐことが可能である。理解を助けるために、どのようにして不正を検出、不正の防止が可能かを具体的な例を示して説明する。

【０１１０】本実施の形態４の再生システムが、航空機やバスなどの移動体において映画上映に用いられている場合を考える。不正の例としては、従業員や客によって許可されないコピーが行われる不正が考えられる。この場合、本実施の形態４の再生システムであれば、不正にコピーされた映像／音声信号から特定された機器、時刻、位置の情報を特定可能であり、さらにその情報と客や従業員の搭乗リストから、不正を行った従業員や乗客を絞り込むことが可能である。あるいは、別の不正の例としては、再生システムを不正に持ち出し、その後に許可されないコピーを行う不正が考えられる。この場合、持ち出されて不正が行われた機器、時刻、位置を特定可能である。また、個人の家で行われた不正についても、その不正を行った機器あるいは住居を特定することができる。

【０１１１】さらに、本実施の形態４によれば、不正した者を特定可能な情報を検出可能であるので、不正をしようとする者に対する不正の抑止効果もある。

【０１１２】なお、本実施の形態４においては、ストリーム送出装置２４０がＭＰＥＧ－ＴＳをストリームとして出力する装置としているが、これに限られるものではなく、以下にストリーム送出装置２４０の他の構成例を

示す。

【０１１３】ストリーム送出装置２４０は、デジタル化された映像信号や音声信号やデータ、あるいはそれらの多重されたストリームを出力する任意の構成の装置である。さらに、ストリームは、映像や音声やデータなどを含む任意のフォーマットのデジタル信号である。ストリームのフォーマットの例としては、ＭＰＥＧ１の映像あるいはＬａｙｅｒ Ｉ、Ｌａｙｅｒ ＩＩ、Ｌａｙｅｒ ＩＩＩ（一般にＭＰ３と呼ばれている）の音声、ＭＰＥＧ２の映像あるいはＢＣ，ＡＡＣの音声、Ｄｏｌｂｙ－ＡＣ３の音声などがある。あるいは、これらを多重した、ＭＰＥＧ２のＴＳあるいはＰＳ（プログラム・ストリーム）などがある。あるいは、ＭＰＥＧ４の映像あるいはＡＡＣやＴｗｉｎＶＱなどの音声などがある。あるいは、ＤＶフォーマットの映像や音声などがある。あるいは、アナログの映像や音声を出力することもでき、もちろん、任意のフォーマットを用いることができる。

【０１１４】また、このようなストリームを出力するデータ出力装置２４０の例としては、無線波によって送信される衛星放送や地上波放送などの信号を受信し、受信した信号からストリームを再生して出力するデジタル放送チューナや、同軸や光ファイバなどの有線によって送信されるケーブルＴＶ、衛星放送や地上波放送の再送信、有線放送などの信号を受信し、受信した信号からストリームを再生して出力するデジタル放送チューナがある。あるいは、実施の形態１及び実施の形態２に示したように、ＤＶＤやＣＤ（コンパクト・ディスク）などの光ディスク、光磁気ディスクや磁気ディスク、デジタルＶＨＳやＤＶなどのテープ、ハードディスク、固体メモリなどの記録媒体に記録されている信号からストリームを再生して出力するデータ再生装置がある。あるいは、電話回線やイーサーネット、ＡＴＭなどのネットワークを介して送信される信号を受信し、受信した信号からストリームを再生する受信装置がある。あるいは、前記のような機能を実現するＰＣ（パーソナル・コンピュータ）やプロセッサがある。もちろん上記の例に限られず、ストリームを出力する任意の装置を用いることができる。

【０１１５】上記に示したように、ストリーム送出装置２４０は任意のストリームを出力する任意の構成をとることができる。この場合、復号化手段２３０については、ストリーム送出装置２４０が出力するストリームを復号化可能な任意の構成になる。

【０１１６】なお、ストリーム送出装置２４０からは、暗号化されたストリームがその鍵と多重されて出力されるとしたが、これに限られるものではなく、たとえば、制御手段２１０に記憶された鍵を用いて暗号化する場合には、その鍵が多重されていなくても良い。さらに、暗号化されていないストリームが出力されても良い。これらの場合、制御手段２１０は、それぞれに必要な処理のみを実現することになる。

【０１１７】また、上記の説明においては、ストリーム送出装置２４０とデータ再生装置２００を１対１で接続するような構成としたが、図１４に示したように、１台のストリーム送出装置２４０から出力されたストリームを複数台のデータ再生装置２０１、２０２、２０３で再生するような構成でも良い。また、図１４ではデータ再生装置２００を３台としているが、何台とる構成をとってもよい。さらに、制御手段２１０についてはＩＣカードのような着脱可能な構成としても良く、同様の効果が得られる。

【０１１８】なお、ＩＤ情報は制御手段２１０から出力されても良いし、データ再生装置２００がＩＤ記憶手段を持つような構成としても良く、同様の効果が得られる。また、本実施の形態４においては、実時刻測定手段２２１と実位置測定手段２２２を備えているが、いずれか一方のみを持つような構成でも良い。

【０１１９】（実施の形態５）以下、図１５から図１７を用いて、本発明の請求項２７と請求項２９に記載された実施の形態５について説明する。まず、図１５を用いて、本実施の形態５の再生システムの構成を説明する。図１５は、本実施の形態５の再生システム例を示す構成図である。図１５において、２０４，２０５，２０６はデータ再生装置、２４１，２４２，２４３はストリーム送出装置、２２１は実時刻測定手段、２２２は実位置測定手段である。

【０１２０】本実施の形態５において、実時刻測定手段２２１、実位置測定手段２２２は、本実施の形態３の各装置と同様のものであり、また、ストリーム送出装置２４１，２４２，２４３は実施の形態４のストリーム送出装置２４０と同様のものであるため、説明を省略する。

【０１２１】また、本実施の形態５のデータ再生装置２０４，２０５，２０６は、データ再生装置内に実時刻測定手段２２１、及び実位置測定手段２２２を備えず、外部から入力された実時刻情報、及び実位置情報を用いる点のみ、実施の形態４のデータ再生装置２００と異なる。

【０１２２】上記の構成により、本実施の形態５は、実施の形態４と同様の効果が得られる。加えて、実時刻測定手段２２１および実位置測定手段２２２の数を削減できる効果や、各データ再生装置での実位置情報や実時刻情報の精度のばらつきをなくせるというさらなる効果がある。

【０１２３】また、データ再生装置２０４、２０５、２０６を、正しい実時刻情報および実位置情報が入力された時にのみ再生動作を行うような構成にすることにより、実時刻情報および実位置情報が埋め込まれずに再生されるような不正や誤動作を防ぐことができる。

【０１２４】これによれば、ストリーム送出装置２４０と各データ再生装置２０４、２０５、２０６が盗まれた

場合に、盗まれた機器による再生を防止することができる。例えば、航空機やバスなどの各座席に機器を貸し出すような場合に、実時刻測定手段２２１および実位置測定手段２２２からの信号を接続しなければ各機器が再生動作しないようにすることにより、貸し出した機器を持ち出しても再生できず、不正な再生を防止できる。

【０１２５】データ再生装置２０４、２０５、２０６において、正しい実時刻情報および実位置情報が入力された時にのみ動作するように制御する方法としては、任意の構成によって実現できる。最も簡単な例としては、実時刻情報および実位置情報が入力された時にのみ再生動作を行う方法がある。さらに、安全性をたかめる実現例としては、実時刻情報および実位置情報に誤り訂正符号や暗号による署名を付加する方法や、暗号による認証を行う方法がある。また、ストリームを復号する鍵情報を実時刻情報および実位置情報と共に伝送する方法によっても実現可能である。このような、実時刻情報および実位置情報が入力されなければ映像／音声信号を再生しないような任意の構成によって実現できる。また、これらの制御はデータ再生装置の制御手段が行うものとしてもよい。

【０１２６】次に図１６を用いて、本実施の形態５における別の再生システムついて説明する。図１６は、本実施の形態５の再生システムにおいて、ストリーム送出装置が１台の場合における再生システムの構成例を示す図である。図１６に示すように、一台のストリーム送出装置２４０から送出されるストリームを複数台のデータ再生装置２０４，２０５，２０６で再生するような再生システムを構築する場合には、多重装置２５０によってストリームと実時刻情報と実位置情報を多重して送信し、データ再生装置２００に入力される前に各分離装置２６１、２６２、２６３によってストリームと実時刻情報と実位置情報に分離するような構成にしても良い。これによれば、伝送に用いる線の数を減らすことができるという効果が生じる。ここで、多重装置２５０によって実時刻情報と実位置情報のみを多重するような構成にしても良い。

【０１２７】さらに、本実施の形態５の再生システムは、図１７に示したような構成でも良い。図１７は、本実施の形態５における再生システムの構成例である。図１７によれば、復号化手段２３１がストリーム中に埋め込まれた情報から時刻などを示す情報を抜き出してタイミング情報を出力し、制御手段２１１がタイミング情報を制御情報送出装置２７０の送信手段２７１を介して鍵送出手段２７２に送信する。鍵送出手段２７２は、そのタイミング情報から鍵の送出タイミングを計算し、暗号化された鍵を出力する。送信手段２７１は、該暗号化された鍵と、実時刻測定手段２２１より出力された実時刻情報と、実位置測定手段２２２より出力された実位置情報を、データ再生装置２０７の制御手段２１１に送信する。制御手段２１１は受信した暗号化された鍵から鍵を生成して、復号化手段２３１に出力する。同時に、受信した実時刻情報と実位置情報を情報埋め込み手段２２０に出力する。これによれば、実時刻情報および実位置情報の入力が無ければ、暗号化を復号するための鍵を入手できず、ストリームの再生ができない。なお、本実施の形態５においては、実時刻測定手段２２１と実位置測定手段２２２を備えているが、いずれか一方のみを持つような構成でも良い。

【０１２８】

【発明の効果】以上のように、本発明の請求項１に記載の鍵記憶装置によれば、本発明の請求項１記載のデータ再生装置は、復号鍵で暗号化された暗号化コンテンツを、デジタルメディアより読み出し、鍵記憶装置に記憶されている前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、前記デジタルメディアの再生状況を監視する再生状況取得手段と、前記復号鍵を用いて前記暗号化コンテンツを復号化するコンテンツ復号化手段とを備え、前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツを、保持した前記復号鍵を用いて、前記コンテンツ復号化手段により復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたので、鍵の不正使用を防止し、再生資格のない再生装置でのコンテンツの再生を防止できる。

【０１２９】また、本発明の請求項２に記載のデータ再生装置によれば、請求項１記載のデータ再生装置において、前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたので、再生装置による再生状況を常に監視でき、再生状態が停止である場合に鍵を破棄し、鍵の不正使用を防止することができる。

【０１３０】また、本発明の請求項３に記載のデータ再生装置によれば、請求項1または請求項２記載のデータ再生装置において、前記デジタルメディアはＤＶＤであるので、ＤＶＤを再生する際、再生資格のない再生装置で、ＤＶＤ内のコンテンツの再生を防止できる。

【０１３１】また、本発明の請求項４に記載のデータ再生装置によれば、コンテンツ鍵で暗号化された暗号化コンテンツと、復号鍵で暗号化された暗号化コンテンツ鍵とを、デジタルメディアより読み出し、鍵記憶装置に記憶された前記復号鍵を用いて再生するデータ再生装置であって、前記鍵記憶装置との間で相互認証を行い、該鍵記憶装置に記憶された復号鍵を取得する鍵取得手段と、該復号鍵を保持する鍵保持部と、前記デジタルメディア

の再生状況を監視する再生状況取得手段と、前記復号鍵を用いて、前記暗号化コンテンツ鍵を前記コンテンツ鍵に復号化する暗号化コンテンツ鍵復号化手段と、前記コンテンツ鍵を用いて、前記暗号化コンテンツを復号化する暗号化コンテンツ復号化手段とを備え、前記鍵取得手段により前記復号鍵を取得して前記鍵保持部に保持し、前記デジタルメディアより読み出した前記暗号化コンテンツ鍵を、保持した前記復号鍵を用いて、前記コンテンツ鍵復号化手段により復号化して前記コンテンツ鍵を取得し、該コンテンツ鍵を用いて、前記デジタルメディアから読み出した前記暗号化コンテンツを復号化して再生し、前記再生状況取得手段によって得た前記デジタルメディアの再生状況に応じて、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたので、鍵の不正使用を防止し、再生資格のない再生装置でのコンテンツの再生を防止することができる。

【０１３２】また、本発明の請求項５に記載のデータ再生装置によれば、請求項４記載のデータ再生装置において、前記再生状況取得手段により、前記デジタルメディアの再生状況が停止であることを確認した時点で、前記鍵保持部に保持していた前記復号鍵を破棄するようにしたので、再生装置による再生状況を常に監視でき、再生状態が停止になった場合に鍵を破棄し、鍵の不正使用を防止することができる。

【０１３３】また、本発明の請求項６に記載のデータ再生装置によれば、請求項４または請求項５記載のデータ再生装置において、前記デジタルメディアはＤＶＤであるようにしたので、ＤＶＤを再生する際、再生資格のない再生装置でのＤＶＤ内のコンテンツの再生を防止できる。

【０１３４】また、本発明の請求項７に記載の鍵記憶装置によれば、デジタルメディアに記録されている、暗号化されたデータを復号化する復号鍵を記憶している復号鍵記憶手段と、該暗号化データを再生する際に、外部装置へ前記復号鍵の読み出し許可を与える鍵読み出し許可手段と、前記復号鍵の外部装置への読み出し実績を記録する鍵読み出し履歴記録手段とを備えた鍵記憶装置であって、前記復号鍵は、該復号鍵の読み出し有効期間である有効期間情報を含み、前記鍵読み出し許可手段は、前記外部装置から前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻を含む鍵要求信号を受け取り、前記鍵読み出し時刻が、前記鍵読み出し履歴記録手段により記録された前記復号鍵の鍵読み出し履歴情報のうちのもっとも新しい時刻よりも後の時刻であることと、前記鍵要求時刻が前記鍵の読み出し有効期間内にあることと、前記鍵読み出し履歴記録手段により前記鍵読み出し履歴情報が記録されたこととを確認したうえで、該外部装置に前記復号鍵の読み出し許可を与えるものであるようにしたので、有効期間付きの鍵について、その申告時刻を逆進させる不正を防止し、鍵の不正取得を防止することができる。

【０１３５】また、本発明の請求項８に記載の鍵記憶装置によれば、請求項７記載の鍵記憶装置において、前記鍵読み出し履歴記録手段は、前記鍵読み出し履歴情報に加えて、該鍵読み出し履歴情報の改ざん検出可能な改ざん検出コードをさらに生成し記録するようにしたので、鍵読み出し履歴情報を改ざんするのを困難にすることができる。

【０１３６】また、本発明の請求項９に記載の鍵記憶装置によれば、請求項７または請求項８記載の鍵記憶装置において、前記鍵読み出し許可手段は、前記鍵読み出し履歴情報に付け加えられた前記改ざんコードより、前記鍵読み出し履歴情報に改ざんがないことを確認し、前記外部装置に前記復号鍵の読み出し許可を与えるようにしたので、鍵読み出し履歴情報の改ざんによる鍵不正使用を防止することができる。

【０１３７】また、本発明の請求項１０に記載の鍵記憶装置によれば、請求項７記載の鍵記憶装置において、前記鍵読み出し履歴記録手段は、所定の記憶容量を持ち、前記鍵読み出し許可手段は、前記鍵読み出し履歴情報が前記鍵読み出し履歴記録手段の前記記憶容量に達した時、前記復号鍵の読み出しを不許可とするようにしたので、鍵へのアクセスに上限を設けることができ、鍵不正使用回数の上限を制限できる。

【０１３８】また、本発明の請求項１１に記載のデータ再生装置によれば、復号鍵で暗号化されたデータを、デジタルメディアより読み出し、再生するデータ再生装置であって、暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置から該復号鍵を取得する鍵取得手段と、前記デジタルメディアから取得した暗号化されたデータを、該復号鍵を用いて復号化する復号処理手段と、前記復号化処理手段により復号化されたデータに情報を埋め込む情報埋め込み手段と、前記データ再生装置の機器識別コードを記憶する機器識別コード記憶手段とを備え、前記鍵取得手段により前記復号鍵を取得し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻及び前記データ再生装置の機器識別コードを、前記情報埋め込み手段により、埋め込み情報として前記復号化されたデータに埋め込むようにしたので、前記鍵読み出し時刻情報及び前記データ再生装置の機器識別コードを、復号化されたデータに埋め込みし、不正者の特定などに利用することができる。

【０１３９】また、本発明の請求項１２に記載のデータ再生装置によれば、請求項１１に記載のデータ再生装置において、前記鍵取得手段は、前記復号鍵を記憶している鍵記憶装置の識別コードを、該鍵記憶装置から前記復号鍵と共に読み出すものであり、前記情報埋め込み手段は、該鍵記憶装置の識別コードを前記埋め込み情報として前記復号化されたデータにさらに埋め込むようにしたので、前記鍵記憶装置の識別コードを、復号化されたデ

ータにさらに埋め込むことができる。

【０１４０】また、本発明の請求項１３に記載のデータ再生装置によれば、請求項１１または請求項１２に記載のデータ再生装置において、前記情報埋め込み手段は、埋め込みパターンを各映像フレーム毎への各埋め込み列に変換する埋め込み列生成手段と、該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換するようにしたので、前記鍵読み出し時刻情報または前記鍵記憶装置の識別コードを、改ざんに強い値列に変換して、復号化されたデータに埋め込みすることができ、また、その埋め込み情報を不正者の特定などに利用することができる。

【０１４１】また、本発明の請求項１４に記載のデータ再生装置によれば、請求項１３に記載のデータ再生装置において、前記鍵取得手段は、前記鍵読み出し時刻及び前記データ再生装置の機器識別コードを含む鍵読み出し履歴信号を生成し、前記復号鍵を保持する鍵記憶装置に伝送するようにしたようにしたので、埋め込み情報と同じ情報を含む鍵読み出し履歴情報を作成することができる。

【０１４２】また、本発明の請求項１５に記載のデジタルコンテンツ再生装置よれば、復号鍵で暗号化されたデータを、デジタルメディアから読み出し、再生するデジタルコンテンツ再生装置であって、暗号化されたデータを再生する復号鍵を記憶する鍵記憶手段と、前記鍵記憶手段から該復号鍵を読み出して再生処理するデータ再生手段とを備え、前記データ再生手段と前記鍵記憶手段との接続は、着脱可能であって、前記鍵記憶手段は、前記データ再生手段が前記復号鍵を読み出したとき、前記デジタルコンテンツ再生装置の機器識別コードと、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻とを含む鍵読み出し履歴情報を記録し、前記データ再生手段は、前記復再生用鍵を用いて再生される再生データに、前記鍵読み出し時刻及び前記デジタルコンテンツ再生装置の機器識別コードを埋め込み情報として埋め込むようにしたので、前記鍵読み出し時刻情報及び該デジタルコンテテンツ再生装置の機器識別コードを、復号化されたデータに埋め込むことができる。

【０１４３】また、本発明の請求項１６に記載のデジタルコンテンツ再生装置によれば、請求項１５記載のデジタルコンテンツ再生装置において、前記埋め込み情報は、各映像フレーム毎への埋め込み列に変換されて電子透かし埋め込みされ、前記埋め込み列は、各映像フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを１ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させたものであるようにしたので、前記鍵読み出し時刻情報及び該デジタルコンテンツ再生装置の機器識別コードを、改ざんに強い値列に変換し、復号化されたデータに電子透かし埋め込みすることで、不正者の特定などに利用することができる。

【０１４４】また、本発明の請求項１７に記載の鍵読み出し履歴記録方法によれば、暗号化データの復号鍵の読み出し有効期間である有効期間情報を記録し、前記復号鍵の読み出し要求がされた時刻である鍵読み出し時刻と該鍵読み出し時刻に最も近い以前の時刻に記録された時刻との差を鍵未使用期間として記録し、前記鍵読み出し時刻及びデータ再生装置の機器識別コードとを含む鍵読み出し履歴情報を記録し、前記復号鍵の使用を終了した時刻を鍵使用終了時刻として記録するようにしたので、時刻情報の逆進を防止でき、さらに鍵の不正使用を防止できる。

【０１４５】また、本発明の請求項１８記載の情報埋め込み装置によれば、埋め込みパターンを各映像フレーム毎への埋め込み列に変換する埋め込み列生成手段と、該埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備え、前記埋め込み列生成手段は、前記埋め込みパターンを、各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、前記埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた前記埋め込み列に変換するようにしたので、改ざんに強い埋め込みパターンを作成できる情報埋め込み装置を提供できる。

【０１４６】また、本発明の請求項１９記載の情報埋め込み装置によれば、現在の時刻を特定可能な実時間情報を出力する実時刻測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入力された時点の前記実時刻情報を埋め込む情報埋め込み手段とを備えるようにしたので、不正が行われた時点の時刻情報が特定可能な映像／音声データを出力でき、その時刻情報により不正者の特定等を行うことができる。

【０１４７】また、本発明の請求項２０記載の情報埋め込み装置によれば、現在の物理的な位置を特定可能な実位置情報を出力する実位置測定手段と、視聴可能な形態で当該装置に入力される映像／音声データに、該映像／音声データが入力された時点の前記実位置情報を埋め込む情報埋め込み手段とを備えるようにしたので、不正が

行われた時点の位置情報が特定可能な映像／音声データを出力でき、その位置情報により不正者の特定等を行うことができる。

【０１４８】また、本発明の請求項２１記載の情報埋め込み方法によれば、現在の時刻を特定可能な実時刻情報を出力する実時刻測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実時刻測定ステップから得られた実時刻情報を埋め込むようにしたので、不正が行われた時点の時刻情報が特定可能な映像／音声データを出力でき、その時刻情報により不正者の特定等を行うことができる。

【０１４９】また、本発明の請求項２２記載の情報埋め込み方法によれば、現在の位置を特定可能な実位置情報を出力する実位置測定ステップと、映像／音声情報に情報を埋め込む情報埋め込みステップとを有し、視聴可能な形態で入力される前記映像／音声データに、該映像／音声データが入力される時点における、前記実位置測定ステップから得られる実位置情報を埋め込むようにしたので、不正が行われた時点の位置情報が特定可能な映像／音声データを出力でき、その位置情報により不正者の特定等を行うことができる。

【０１５０】また、本発明の請求項２３記載の埋め込み情報検出装置は、埋め込みパターンを各フレームに埋め込めるビット数に応じて分割して埋め込む短周期埋め込みパターンと、埋め込みパターンを1ビットずつに分割し、該分割した値を複数フレームにわたって埋め込み、前記埋め込みパターンの分割した数の複数倍のフレームを用いて埋め込む長周期埋め込みパターンとを混在させた埋め込み列を生成する埋め込み列生成手段と、前記埋め込み列を各映像フレームに電子透かし埋め込みする埋め込み手段とを備える情報埋め込み装置によって、埋め込み情報を埋め込まれた再生データから、前記埋め込み情報を検出する埋め込み情報検出装置であって、該埋め込み情報検出装置は、各映像フレームから埋め込みパターンを検出するフレーム内埋め込み情報検出手段と、前記フレーム内埋め込み情報検出手段が検出する埋め込みパターンより、短周期埋め込みビットを参照して埋め込みパターンを算出する短周期埋め込みパターン検出手段と、長周期埋め込みビットを参照して埋め込みパターンを算出する長周期埋め込みパターン検出手段とを備えるようにしたので、情報埋め込み装置で埋め込みパターンを長周期及び短周期パターンを利用した改ざんに強い埋め込みパターン列に変換して埋め込められた埋め込み情報を検出することができる。

【０１５１】また、本発明の請求項２４記載の埋め込み情報確認方法によれば、現在の時刻を特定可能な実時刻情報、現在の位置を特定可能な実位置情報または、視聴可能なデータのうちの少なくとも１つを再生する装置の

機器識別コードを埋め込み情報として埋め込んだ前記視聴可能なデータより、該埋め込み情報を検出し、前記埋め込み情報の履歴である情報埋め込み履歴データベースと、検出した前記埋め込み情報とを照合処理するようにしたので、記録された履歴データベースと、検出した前記埋め込み情報を突き合わせることができ、不正者への追跡性をより高くすることができる。

【０１５２】また、本発明の請求項２５記載の埋め込み情報確認方法によれば、請求項２４記載の埋め込み情報確認方法において、前記埋め込み情報は、暗号化されたデータを含むデジタルメディアを再生するデータ再生装置の機器識別コード、及び該暗号化されたデータを復号化する復号鍵を記憶する鍵記憶装置に、前記復号鍵の読み出し要求した時刻である鍵読み出し時刻であり、前記埋め込み履歴データベースは、前記復号鍵の前記データ再生装置への読み出し実績を記録する鍵読み出し履歴記憶手段を回収したものであるようにしたので、鍵の使用を記録した鍵使用履歴記憶部の情報と埋め込み情報とを突き合わせることができ、不正者の追跡性をより高めることができる。

【０１５３】また、本発明の請求項２６記載の再生システムによれば、データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の時刻を特定可能な実時刻情報を出力する実時刻測定手段と、前記映像／音声データに情報を埋め込む情報埋め込み手段とを備え、前記データ再生装置が前記入力されるデータを再生した時点における前記実時刻測定手段による前記実時刻情報を埋め込むようにしたので、復号化して視聴可能な映像／音声信号に、不正が行われた時点の時刻情報を埋め込むことができ、その埋め込まれた時刻情報により、不正者の特定等を行うことができる。

【０１５４】また、本発明の請求項２７記載の再生システムによれば、請求項２６記載の再生システムにおいて、一台の前記実時刻測定手段と、少なくとも一台の前記データ出力装置とを備えるようにしたので、複数の再生装置を有するシステムにおいて映像／音声信号に埋め込む時刻情報を不正者の特定などに利用でき、また複数の再生装置間での時刻情報のばらつきをなくせ、伝送に用いる配線を少なくすることができる。

【０１５５】また、本発明の請求項２８記載の再生システムによれば、データを出力するデータ出力手段と、データ再生装置とを備える再生システムであって、前記データ再生装置は、入力されるデータを視聴可能な映像／音声データに復号化する復号化手段と、現在の位置を特定可能な実位置情報を出力する実位置測定手段と、前記実位置情報を前記映像／音声データに埋め込む情報埋め込み手段とを備え、前記データ再生装置が前記入力されるデータを再生した時点における前記実位置測定手段に

よる前記実位置情報を埋め込むようにしたので、復号化して視聴可能な映像／音声信号に、不正が行われた時点の位置情報を埋め込むことができ、その埋め込まれた位置情報により、不正者の特定等を行うことができる。

【０１５６】また、本発明の請求項２９記載の再生システムによれば、請求項２８記載の再生システムにおいて、一台の前記実位置測定手段と、少なくとも一台の前記データ出力装置とを備えるようにしたので、複数の再生装置を有するシステムにおいて映像／音声信号に埋め込む位置情報を不正者の特定などに利用でき、また複数の再生装置間での位置情報のばらつきをなくせ、伝送に用いる配線を少なくすることができる。

【図面の簡単な説明】

【図１】本発明の実施の形態１におけるデータ再生装置の一構成例を示す図である。

【図２】本発明の実施の形態１におけるデータ再生装置の動作例を示すフローチャート図である。

【図３】本発明の実施の形態１におけるデータ再生装置が不正なものとして判断された場合のブロック線図である。

【図４】本発明の実施の形態２におけるデータ再生装置及び鍵記憶装置を含むシステムの一構成例を示すブロック図である。

【図５】本発明の実施の形態２におけるデータ再生装置及び鍵記憶装置が再生処理を行う場合の動作例を示すフローチャート図である。

【図６】本発明の実施の形態２における履歴情報記入例を示す図である。

【図７】本発明の実施の形態２における履歴情報記入の処理手順例を示すフローチャート図である。

【図８】本発明の実施の形態２における電子透かし埋め込み処理部の構成及びその埋め込み情報検出装置の構成を示す図である。

【図９】本発明の実施の形態２における電子透かし埋め込み処理の結果、各フレームに埋め込められるパターン列を示す図である。

【図１０】本発明の実施の形態２における記録された履歴情報を、不正機器、不正鍵記録装置または不正を行った時刻の特定をする場合に利用する時の装置構成例を示す図である。

【図１１】本発明の実施の形態３における情報埋め込み手段の構成を示す図である。

【図１２】本発明の実施の形態３における埋め込まれた情報の検出処理を行う場合の構成例を示した図である。

【図１３】本発明の実施の形態４における再生システムの構成を示す図である。

【図１４】本発明の実施の形態４における再生システムにおいて、再生装置を複数もつ場合の再生システムの構成を示す図である。

【図１５】本発明の実施の形態５における再生システムの一構成例を示す図である。

【図１６】本発明の実施の形態５における再生システムの一構成例を示す図である。

【図１７】本発明の実施の形態５における再生システムの一構成例を示す図である。

【図１８】本発明の従来例であるデータ再生装置の構成を示す図である。

【符号の説明】

１０ａ，１０ｂ，４０　鍵記憶装置
１１ａ，１１ｂ，４１　鍵記憶装置内の制御部
１２ａ，１２ｂ　鍵記憶部
２０，２３，２６　ＤＶＤ
２１，２４，２７，３１　暗号化コンテンツ鍵
２２，２５，２８，３２　暗号化コンテンツ
３０　記録メディア
４２，１１２　再生用装置鍵記憶部
４３　有効期間記憶部
４４　履歴情報記録部
４５，１１５　コンテンツ識別コード記憶部
４６，１１６　時刻情報記憶部
４７，１１７　再生装置識別コード記憶部
４８，１１８　鍵記憶装置識別コード記憶部
４９，１１９　鍵記憶装置／再生装置間鍵記憶部
５０　鍵管理部
５１　コンテンツ暗号化部
５２　データ暗号化部
５３　時計
６０　不正に複製された記録メディア
１００　ＤＶＤプレーヤ
１０１　制御部
１０２　コンテンツ鍵復号鍵保持部
１０３　暗号化コンテンツ鍵復号化部
１０４　読み出し部
１０５　暗号化コンテンツ復号化部
１０６　再生部
１０７　信号出力部
１０８　ユーザ操作入力部
１１０　データ再生装置
１１１　制御部
１１３　鍵復号処理部
１１４　再生処理部
１２０　電子透かし埋め込み処理部
１２１　埋め込みシーケンス生成部
１２２　電子透かし埋め込み処理部
１２３　短周期埋め込みパターン検出部
１２４　長周期埋め込みパターン検出部
１２５　電子透かし検出部
１３１　電子透かし情報検出装置
１３２　再生装置識別コードによる検索検証処理
１３３　鍵記憶装置識別コードによる検索検証処理

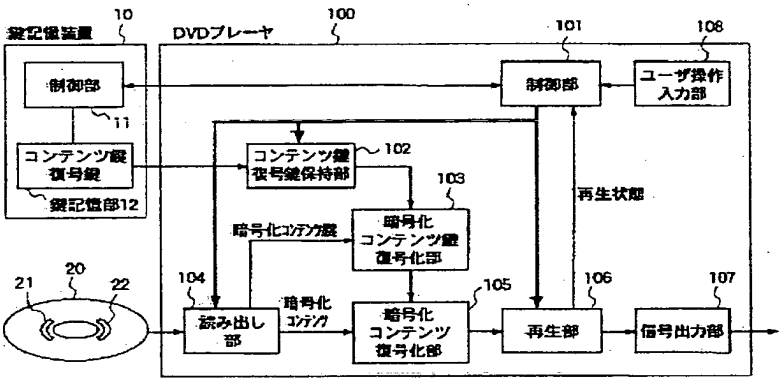
45

１３４　読み出し時刻情報により検索検証処理
２００，２０１，２０２，２０３，２０４，２０５，２０６，２０７　データ再生装置
２１０，２１１　制御手段
２２０　情報埋め込み手段
２２１　実時刻測定手段
２２２　実位置測定手段
２２３　ＩＤ記憶手段
２３０，２３１　復号化手段
２４０，２４１，２４２，２４３　ストリーム送出装置
２５０　多重装置
２６１，２６２，２６３　分離装置
２７０　制御情報送出装置
２７１　送信手段
２７２　鍵送出手段
２８０　情報検出手段

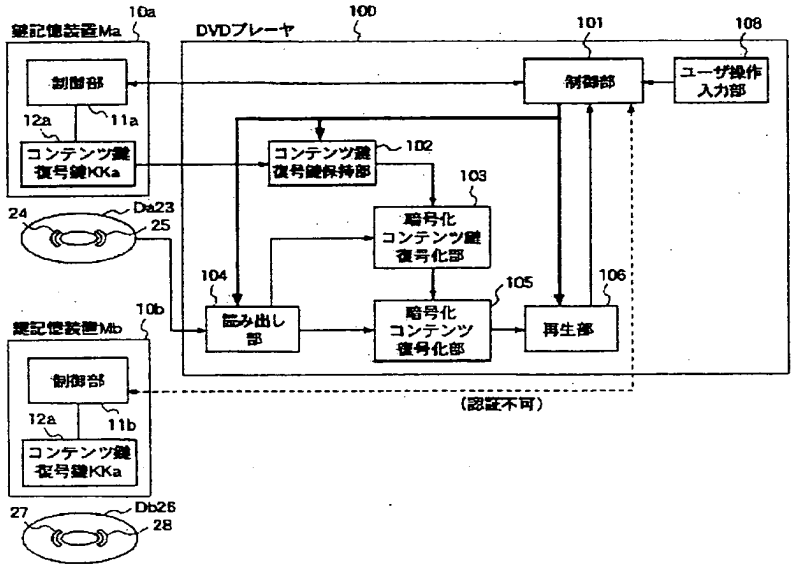
46

２８１　照合手段
２８２　データベース
１０００　鍵記憶装置
１００１　制御部
１００２　鍵記憶部
１１００　データ再生装置
１１０１　制御部
１１０２　コンテンツ鍵保持部
１１０４　読み出し部
１１０５　暗号化コンテンツ復号化部
１１０６　再生部
１１０７　信号出力部
１１０８　ユーザ操作入力部
１２００　デジタルメディア
１２０２　暗号化コンテンツ

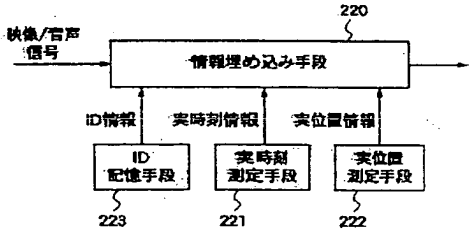
【図１】



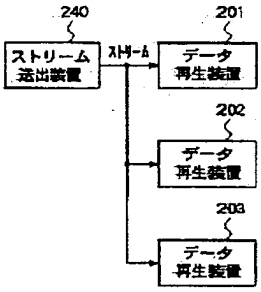
【図３】



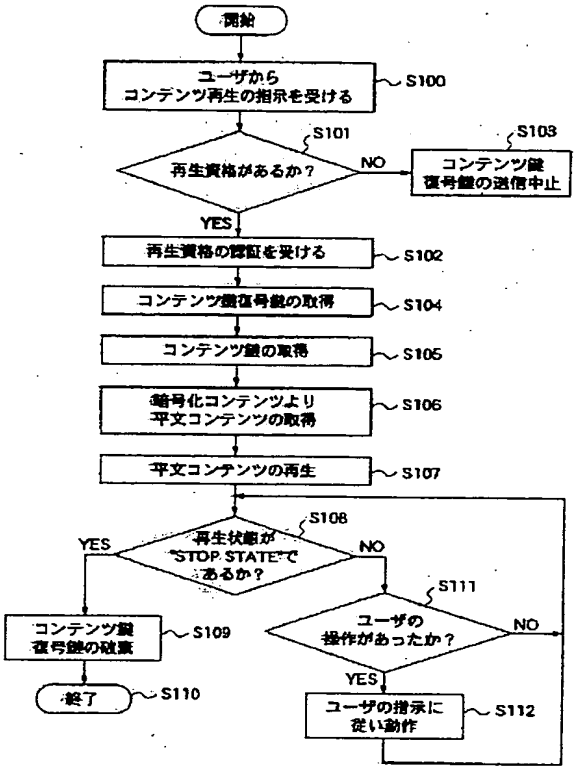
【図１１】



【図１４】



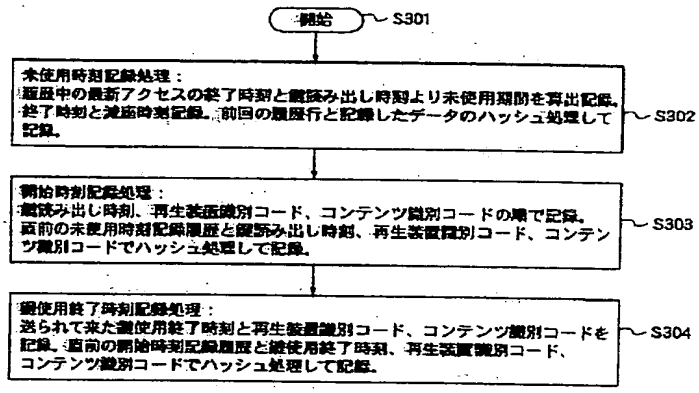
【図２】



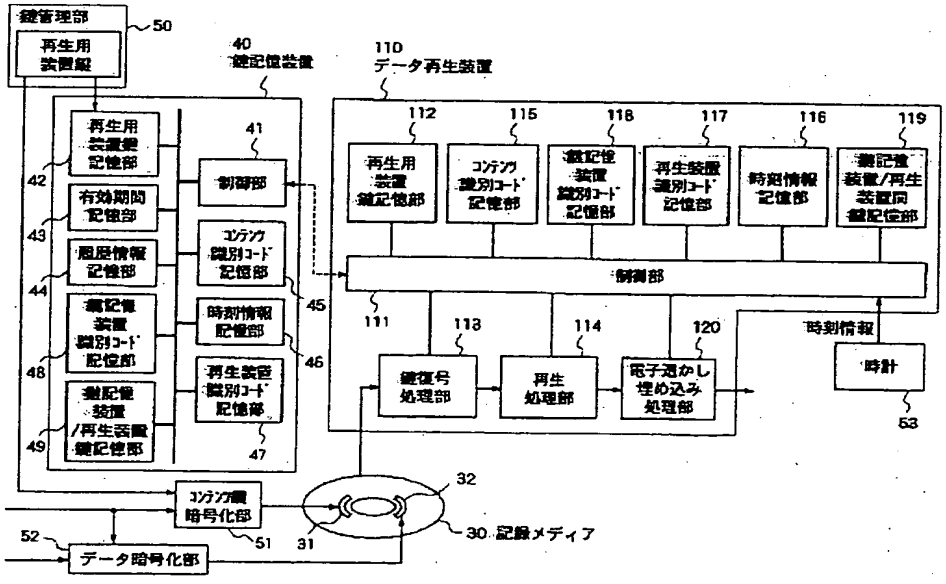
【図６】

鍵有効時刻			ハッシュ値1
未使用期間	鍵有効時刻	開始時刻1	ハッシュ値2
開始時刻1	再生装置識別コード1	コンテンツ識別コード1	ハッシュ値3
終了時刻1	再生装置識別コード1	コンテンツ識別コード1	ハッシュ値4
未使用期間	終了時刻1	開始時刻2	ハッシュ値5
開始時刻2	再生装置識別コード2	コンテンツ識別コード2	ハッシュ値6
終了時刻2	再生装置識別コード2	コンテンツ識別コード2	ハッシュ値7

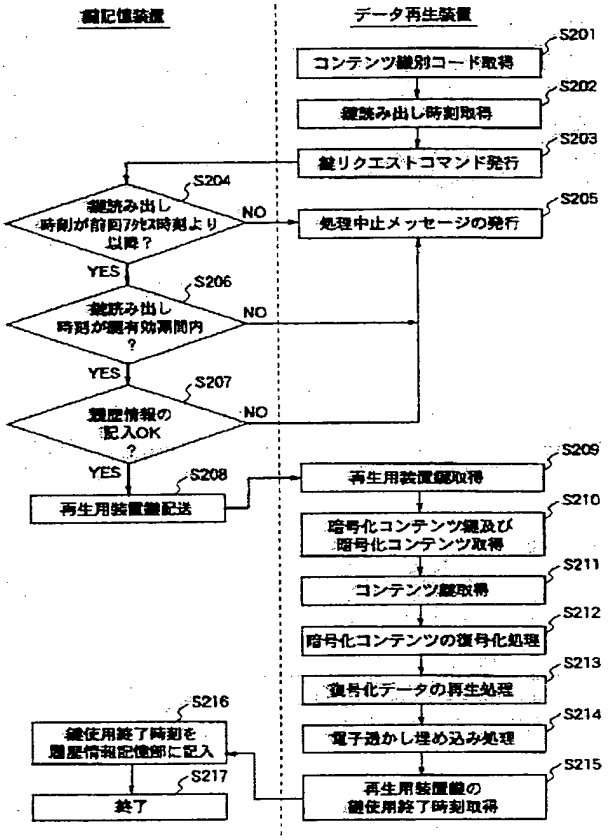
【図７】



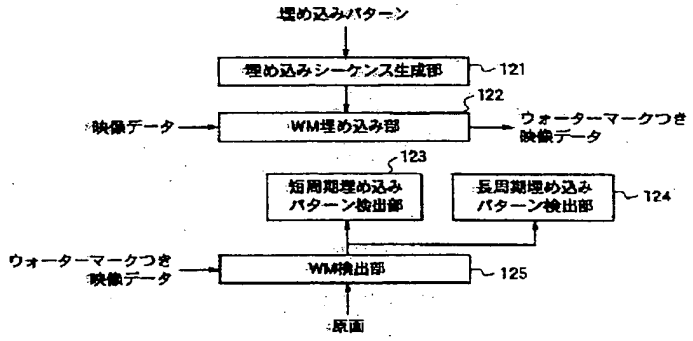
【図４】



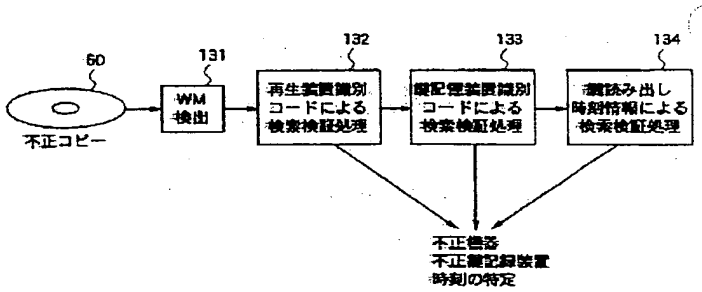
【図５】



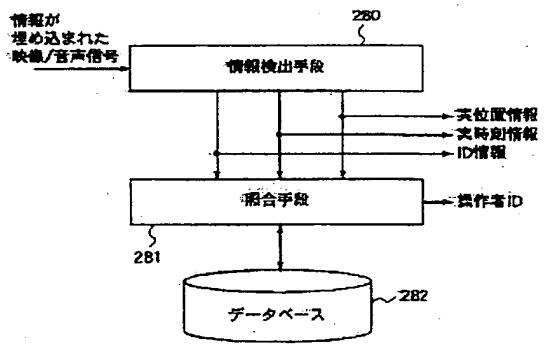
【図８】



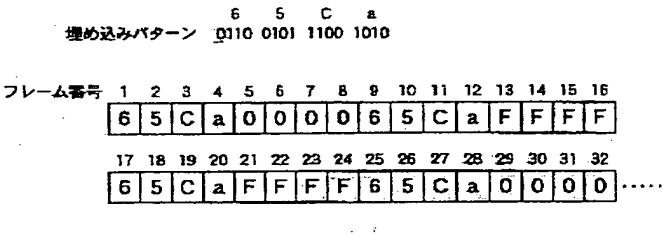
【図１０】



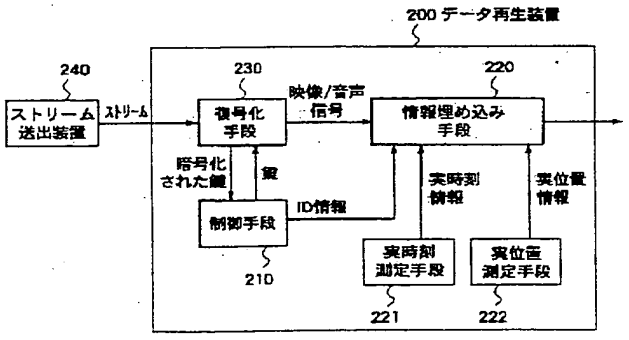
【図１２】



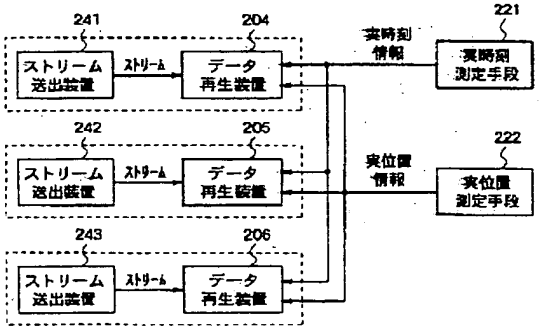
【図９】



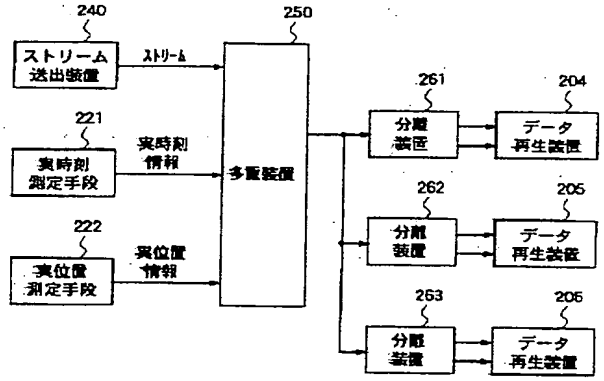
【図１３】



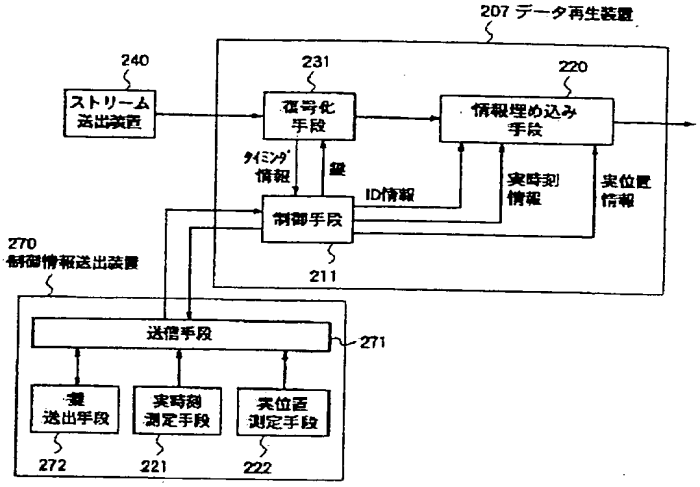
【図１５】



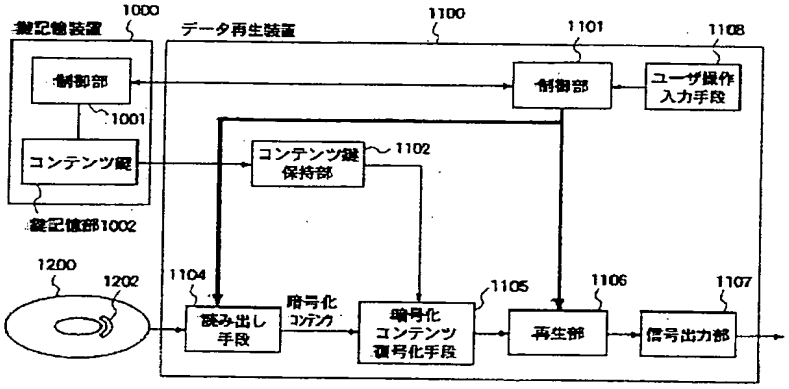
【図１６】



【図１７】



【図１８】



フロントページの続き

(51)Int.Cl.⁷	識別記号	F I	ﾃｰﾏｺｰﾄﾞ(参考)
		H04L 9/00	601E

(72)発明者　茨木　晋
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　館林　誠
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(72)発明者　原田　俊治
大阪府門真市大字門真1006番地　松下電器産業株式会社内